Математички факултет

Универзитета у Београду

Смер: Професор наставе математике и рачунарства

ДЕЉИВОСТ И ФАКТОРИЗАЦИЈА У ШКОЛИ

-МАСТЕР РАД-

Ментор:
Проф. Др Александар Липковски

Студент:
Марија Зејак

Београд, 2017. године

САДРЖАЈ

ПРЕДГОВОР

Рад је подељен на три поглавља: Дељивост, Прости бројеви и Конгруенције. Свако поглавље бави се теоријском обрадом појмова који се уче у склопу редовне и додатне наставе, са освртом на карактеристичне примере. Примери и задаци прате и илуструју дефиниције и теореме у раду. Такође, у сваком поглављу налазе се неке од примена из ових области, које се могу радити како на секцији, тако и на додатној и допунској настави.

Рад не обухвата сву теорију потребну за припрему за такмичење, али првенствено није ни намењен томе. Како нису сва деца која су заинтересована за математику уједно заинтересована за такмичење, идеја рада је да на једном месту обједини основне појмове из области дељивости и факторизације, примере и примене које ће помоћи деци да се више заинтересују, да боље разумеју и да продубе своја знања. Управо због тога, градиво које је обрађено у раду могло би се користити на часовима математчке секције, јер на часовима додатне наставе време дозвољава да се одради само теоријски минимум који је потребан за израду задатака и углавном се раде задаци који су се појављивали на такмичењима, а на часовима математичке секције се могу детаљније обрађивати наведене области.

У раду се инсистира на доказима, јер сматрам да су једноставни и разумљиви за ученике осмог разреда. У доказивању се обично позивамо на претходно доказано тако да морају да повезују градиво и тиме побољшају размишљање, а и да у каснијем школовању лакше разумеју теже доказе.

Задаци из ових области су интересантни свим ученицима, како бољим ђацима тако и оним мање добрим, захтевају размишљање, креативност и помажу у развијању логичког размишљања.

1 ДЕЉИВОСТ

Са дељивошћу бројева ученици се сусрећу у нижим разредима основне школе. У првом разреду формира се појам дељења преко растављања скупова на једнакобројне дисјунктне подскупове, а затим се повеже да је то операција супротна множењу.
За непознату се узима или број таквих подскупова или број елемената у сваком од њих.
Пример. 12 жетона треба поделити једнако на три ученика. По колико жетона ће добити сваки ученик (12 жетона треба поделити једнако и то по 4 жетона сваком ученику. Колико ће ученика добити жетоне)?
Решење. Растављају скуп од 12 жетона на три једнакобројна подскупа: узимају три жетона и стављају по један жетон на три места док се не узму сви жетони из скупа. Симболички исказан одговор: $12 : 3 = 4$.
Одмах усвајају појмове дељеник, делилац и количник и прелазе на везу множења и дељења.
Пример. Упоредимо записе $12{:}\,3 = 4$ и $4 \cdot 3 = 12$.
Ако помножимо количник и делилац добијамо дељеник. Дакле, поделити број 12 бројем 3 значи наћи број којим треба помножити број 3 да се добије 12 (наћи број којим треба помножити делилац да се добије дељеник).
Након тога формирају таблицу дељења (преко таблице множења) и тиме се истиче правило дељења бројевима 1 и 0:

- $a{:}\,1 = a$, јер је $a \cdot 1 = a$.
- Нула је дељеник: $0{:}\,a = 0$, јер је $0 \cdot a = 0$.
- Нула је и дељеник и делилац: $0{:}\,0 = a$, јер је $a \cdot 0 = 0$, где је a било који број.
- Нула је дељеник: нулом се не дели - $a{:}\,0$ није могуће извести јер не постоји број који помножен нулом даје број a.

Ученици се такође упознају са случајем када дељеник није дељив делиоцем (7 жетона треба поделити једнако на три ученика), формирају појам остатка и дељења са остатком. Можда би овде требало нагласити да ће у каснијим разредима учити како да „наставе“ дељење, јер у петом разреду ученик, на пример, приликом дељења $7{:}\,3$ заустави се код остатка и има потешкоћу да настави дељење (у сећању им је остало да то није могуће).
Особине дељивости које упознају:

- Дељење збира бројем:

$(a + b){:}\,c = a{:}\,c + b{:}\,c$, бројеви a и b морају бити дељиви са c. Односно, збир је дељив неким бројем ако су сабирци дељиви са тим бројем. Сабирци не морају бити дељиви неким бројем да би збир био дељив тим бројем.

- Дељење разлике бројем:

$(a - b){:}\,c = a{:}\,c - b{:}\,c$, бројеви a и b морају бити дељиви са c. Умањеник и умањилац не морају бити дељиви неким бројем да би разлика била дељива тим бројем.

Ово су својства на која се враћамо у петом разреду, приликом испитивања дељивости неким бројем[1]. Потребно је направити фину везу између ових записа и коришћења симбола $\mid$ - „дели“, како би умели да искористе научено знање, а не да мисле да уче нешто потпуно ново.

[1] Нећемо овде наводити и својства множења.

- Зависност количника од промене дељеника:

Нека је $a:b=k$, онда је $(a\cdot n):b=k\cdot n$, односно, ако дељеник повећамо n пута, тада се количник повећа n пута.
Нека је $a:b=k$, онда је $(a:n):b=k:n$, односно, ако дељеник смањимо n пута, тада се количник смањи n пута.

- Зависност количника од промене делиоца:

Нека је $a:b=k$, онда је $a:(b\cdot n)=k:n$, односно, ако делилац повећамо n пута, тада се количник смањи n пута.
Нека је $a:b=k$, онда је $a:(b:n)=k\cdot n$, односно, ако делилац смањимо n пута, тада се количник повећа n пута.

- Сталност количника:

Нека је $a:b=k$, онда је $(a\cdot n):(b\cdot n)=k$, или $(a:n):(b:n)=k$.
Количник два броја остаје непромењен ако дељеник и делилац смањимо исти број пута, односно, повећамо исти број пута.

Како ова својства ученици брзо забораве, на њих би се могли вратити након наставне теме Разломци и показати како да лако провере својства преко разломака.

Поред овога у нижим разредима основне школе уче се и критеријуми дељивости бројевима 2, 5 и 10.

Овде бих још истакла да ученици реченицу „прво радимо множење и дељење па сабирање и одузимање “ схватају да множење има предност над дељењем, као и сабирање над одузимањем, па би у нижим разредима требало обратити више пажње на то.

Наставна тема Дељивост је прва из области алгебре која се изучава у петом разреду. Знања из ове области су неопходна за усвајање наставне теме Разломци. Осим повезаности са разломцима, ова тема је релативно слабо повезана са осталим садржајима математике у основној школи. Јавља се у седмом разреду - растављање бројева на просте чиниоце (може бити веома корисно приликом израчунавања квадратних корена бројева, коришћењем појединих особина дељивости доказује се ирационалност квадратних корена простих бројева).
Ученици се први пут сређу са теоремама и доказима (додатна настава) из области теорије бројева. Иако је неопходно образложити зашто је неко тврђење тачно, нагласак се ставља на формулације и примене - основне особине дељивости, критеријуми дељивости и тако даље.

1.1 Појам дељивости бројева

Уочимо да су операције сабирања, одузимања и множења неограничено изводљиве у скупу $\mathbb{Z}$, док са операцијом дељења то није случај. У општем случају није могуће, без остатка, поделити сваки цео број било којим другим целим бројем. Могућност, односно немогућност дељења целих бројева без остатка представља однос међу бројевима назван дељивост.
Напоменимо да се у петом разреду, при разматрању дељивости, ограничавамо на ненегативне целе бројеве. А то се лако преноси на скуп целих бројева јер ако $a\mid b$, очигледно је да $a\mid(-b),(-a)\mid b,(-a)\mid(-b)$.

Дефиниција 1. Цео број a **дељив је** целим бројем b, различитим од нуле, ако постоји цео број q такав да је $a = bq$, тј. ако је количник $a: b = q$ цео број.

Ако је број a дељив бројем b пишемо $b \mid a$ („b дели a“) . У супротном $b \nmid a$ („b не дели a“).

Кажемо да је b **делитељ (фактор)** броја a, а да је a **садржалац (умножак)** броја b.

Број b називамо **прави делитељ** броја a ако је $b \neq a$.

1.2 Особине релације дељивости

Ако другачије не нагласимо, за сваки број који поменемо подразумеваћемо да је цео.

Теорема 1. 1° $a \mid a$. (рефлексија)

2° Ако $a \mid b$ и $b \mid c$, онда $a \mid c$. (транзитивност)

3° Ако, $a \mid b$ и $a \mid c$ онда $a \mid bx + cy$ за све $x, y \in \mathbb{Z}$. (линеарност)

4° Ако $a \mid b$ и $b \neq 0$, тада је $|a| \leq |b|$.

5° Ако $a \mid b$ и $b \mid a$, онда је $a = b$ или $a = -b$.

6° $1 \mid a$. (сваки број је дељив јединицом)

7° $a \mid 0$. (сваки број дели нулу)

Доказ. На основу дефиниције лако је доказати тврђења.

1° По дефиницији јер $a = a \cdot 1$.

2° Ако $a \mid b$ и $b \mid c$, онда по дефиницији постоје цели бројеви m и n такви да је $b = ma$ и $c = nb$.

Онда је $c = nb = \boldsymbol{nm}a$, где је nm цео број. Следи да $a \mid c$.

3° Ако $a \mid b$ и $a \mid c$, онда постоје цели бројеви m и n такви да је $b = ma$ и $c = na$.

Онда је $bx + cy = max + nay = a(\boldsymbol{mx} + \boldsymbol{ny})$, где је $mx + ny$ цео број.

Следи да $a \mid bx + cy$.

4° Нека је $b = ma$. Одатле следи $|b| = |m| \cdot |a|$. Како је $b \neq 0$, очито је$|m| \geq 1$, па је

$$|b| = |m| \cdot |a| \geq 1 \cdot |a| = |a| > 0.$$

5° ° Ако $a \mid b$ и $b \mid a$, онда на основу тврђења 4° имамо $|b| \leq |a|$ и $|a| \leq |b|$, па следи да је $|a| = |b|$, одакле следи тврђење.

6° $a = a \cdot 1$.

7° $0 = 0 \cdot a$. □

Последица 1. Релација дељивости је релација поретка на скупу $\mathbb{N}$.

Доказ. Из претходне теореме својства 1°,2°,5°(у $\mathbb{N}$ важи $a = b$). □

Теорема 2. 1° Ако $a \mid b$ и $c \mid d$, онда $ac \mid bd$.

2° Ако $a \mid b$, тада a дели и сваки умножак броја b, тј. $a \mid cb$, за свако $c \in \mathbb{Z}$.

3° Ако $a \mid b$, тада $\frac{b}{a} \mid b$.

4° Ако су бројеви a и b дељиви бројем c, и ако $a \mid b$, онда $\frac{a}{c} \mid \frac{b}{c}$.

Доказ. 1° Ако $a \mid b$ и $c \mid d$ онда постоје цели бројеви m и n такви да је $b = ma$ и $d = nc$. Одатле је

$$bd = manc = mnac, mn \in \mathbb{Z} \Longrightarrow ac \mid bd.$$

2° $a \mid b \Longrightarrow b = am, m \in \mathbb{Z}$,

Одатле је $cb = cam = cma, cm \in \mathbb{Z} \Longrightarrow a \mid cb$.

3° Ако $a \mid b$ онда је $\frac{b}{a}$ цео број.

$a \mid b \Longrightarrow b = ma, m \in \mathbb{Z} \Longrightarrow m = \frac{b}{a} \in \mathbb{Z}.$

Одатле, $b = ma = \frac{b}{a} \cdot a, a \in \mathbb{Z} \Longrightarrow \frac{b}{a} \mid b.$

4° Ако су бројеви a и b дељиви бројем c, онда су бројеви $\frac{a}{c}$ и $\frac{b}{c}$ цели.

Ако $a \mid b$ онда $b = ma, m \in \mathbb{Z}$. Одатле је $\frac{b}{c} = m\frac{a}{c}$, што доказује да $\frac{a}{c} \mid \frac{b}{c}$. □

Теорема 3. 1° Ако $a \mid b$ и $a \mid c$, тада $a \mid (b + c)$ и $a \mid (b - c)$.

2° Ако $a \mid b$ или $a \mid c$, тада $a \mid bc$.

3° Ако $a_i \mid b_i, i = \overline{1,n}$, тада $a_1 a_2 \cdots a_n \mid b_1 b_2 \cdots b_n$.

4° Ако $a \mid b$, тада $a^n \mid b^n$ за свако $n \in \mathbb{N}$.

Доказ. 1° Последица особине линеарности за $x = 1$ и $y = \pm 1$.

2° Нека на пример, $a \mid c$. Тада $c = ma, m \in \mathbb{Z}$.

$$bc = bma, bm \in \mathbb{Z} \Longrightarrow a \mid bc.$$

3° У доказу користимо теорему 2.1° и математичку индукцију.

Тврђење је тачно за $n = 2$, јер на основу поменуте теореме имамо:

$$a_1 \mid b_1 \text{ и } a_2 \mid b_2, \text{ онда } a_1 a_2 \mid b_1 b_2.$$

Нека је тврђење тачно за $n - 1$, докажимо да важи и за n:

Важи

$$a_i \mid b_i, i = \overline{1, n-1} \Longrightarrow a_1 a_2 \cdots a_{n-1} \mid b_1 b_2 \cdots b_{n-1}.$$

Ако је поред тога $a_n \mid b_n$, из претходног имамо

$$(a_1 a_2 \cdots a_{n-1}) a_n \mid (b_1 b_2 \cdots b_{n-1}) b_n, \text{ тј.}$$

$$a_1 a_2 \cdots a_{n-1} a_n \mid b_1 b_2 \cdots b_{n-1} b_n.$$

4° Из претходног за $a_1 = a_2 = \cdots = a_n$ и $b_1 = b_2 = \cdots = b_n$. □

***Задатак* 1.** Не израчунавајући, испитај тачност следећих тврђења:

1) $4 \mid (160 + 44)$

   $4 \mid 160$ и $4 \mid 44 \overset{\text{T.3.1°}}{\Longrightarrow} 4 \mid (160 + 44)$

2) $6 \mid 3 \cdot 12$

   $6 \mid 12 \overset{\text{T.3.2°}}{\Longrightarrow} 6 \mid 3 \cdot 12.$ ◊

Дакле, видели смо да ако су оба сабирка (умањеник и умањилац) дељива неким бројем и збир (разлика) је дељив тим бројем, односно, ако је један од чинилаца дељив неким бројем и производ је дељив тим бројем.

Примедба 1. Обрнута импликација не важи.

Пример. Ако другачије раставимо бројеве из претходног задатка:

- $4 \mid (160 + 44)$, тј. $4 \mid 204$, али број 204 можемо да напишемо као $204 = 201 + 3$, па и даље важи

  $4 \mid (201 + 3)$, али $4 \nmid 201$ и $4 \nmid 3$.
- Исто тако имамо $6 \mid 4 \cdot 9$, али $6 \nmid 4$ а и $6 \nmid 9$.

Дакле, ако сабирци нису дељиви неким бројем не значи увек да и њихов збир није дељив тим бројем. Ако је збир бројева дељив неким бројем, не мора да значи да је сваки од сабирака дељив тим бројем (Аналогно и за производ и разлику).

Теорема 4. Ако се у једнакости облика

$$a_1 + a_2 + \cdots + a_k = 0 \qquad (1)$$

за све сабирке осим једног зна да су дељиви целим бројем c, онда је и тај сабирак дељив са c.

Доказ. Нека за сабирак a_i не знамо да ли је дељив бројем c а за све остале знамо да су дељиви са c. Имамо:

$$a_1 = cb_1, \dots, a_{i-1} = cb_{i-1}, a_{i+1} = cb_{i+1}, \dots, a_k = cb_k,$$

где су $b_1, \dots, b_{i-1}, b_{i+1}, \dots, b_k$ цели бројеви. Но онда једнакост (1) даје

$$a_i = -c(b_1 + \cdots + b_{i-1} + b_{i+1} + \cdots + b_k),$$

тј. $a = cb_i, b_i \in \mathbb{Z}$, што је и требало доказати. □

1.3 Дељење са остатком

У случају да $b \nmid a$, тј. Да $a:b$ није природан број, онда кажемо да делимо са остатком.

Теорема 5. (О дељењу са остатком) Сваки цео број a може се на јединствен начин помоћу датог природног броја b приказати у облику

$$a = bq + r, \quad 0 \le r < b, \quad \text{где су } q, r \in \mathbb{Z}. \qquad (2)$$

При томе се q назива непотпун количник, а r остатак при дељењу броја a бројем b. Ако је $r = 0$, онда је број a дељив бројем b.

Израз (2) можемо још записати

$$a:b = q(r).$$

Доказ. Докажимо најпре да постоје бројеви q и r као у исказу теореме. У ту сврху, размотримо рационалан број $\frac{a}{b}$. Нека је q цео број такав да $\frac{a}{b}$ лежи у полуотвореном интервалу $[q, q+1)$. Очигледно важи $0 \le \frac{a}{b} - q < 1$.

$a = bq + r \Longrightarrow r = a - bq$.

Ставимо $r = a - bq = a \cdot \frac{b}{b} - bq = b \cdot \frac{a}{b} - bq = b\left(\frac{a}{b} - q\right)$. Из претходне неједнакости следи $0 \le r < b$.

Докажимо јединственост тих бројева. Претпоставимо да постоји још један пар (q_1, r_1), такав да је $a = bq_1 + r_1, 0 \le r_1 < b$. Одузимањем ове једнакости од једнакости (2) добијамо

$$0 = a - a = b(q - q_1) + (r - r_1),$$
$$r - r_1 = b(q - q_1),$$
$$\text{односно } b \mid r - r_1.$$

Због $o \le r < b$ и $0 \le r_1 < b$, важи $|r - r_1| < b$ па имамо да је $r - r_1 = 0$, тј. $r = r_1$, а због тога и $q = q_1$. □

Примедба 2: У теореми претпоставка да је b природан број може се заменити са $b \neq 0$, али је онда $0 \le r < |b|$.

Примедба 3: Уместо (2) може се разматрати израз

$$a = bq_1 - r_1, \quad 0 \le r_1 < b,$$

при чему се број r_1 назива **недостатком**.

Пример.

- $737 = 81 \cdot 9 + 8$
  $737 = 82 \cdot 9 - 1$
- $-737 = (-82) \cdot 9 + 1$
  $-737 = (-81) \cdot 9 - 8$

Чињеница да је приликом дељења целог броја a бројем b остатак r означава се и изразом

$$a \equiv r \ (mod\ b),$$

али ћемо се тиме мало више бавити у другом делу рада.

1.4 Највећи заједнички делилац

Дефиниција 2. Делилац неког броја a јесте сваки цео број којим је број a дељив, то јест сваки број којим се broj a може поделити без остатка.
Скуп свих делилаца броја a означавамо са D_a.
Примедба 4. Због особине транзитивности релације дељивости важи: Ако број b дели број a, онда и сви делиоци броја b деле број a.
Пример. Ако је дати број дељив бројем 21, онда је тај број дељив и свим делиоцима броја 21.

Дефиниција 3. Цео број d је **заједнички делилац** бројева a и b ако $d \mid a$ и $d \mid b$.
Сваки цео број различит од нуле има коначно много делилаца, па је према томе и скуп заједничких делилаца два цела броја коначан и у њему постоји највећи број. У складу с тим даје се и
Дефиниција 4. Највећи међу заједничким делиоцима бројева a и b је **највећи заједнички делилац** бројева a и b. Обележавамо га са (a, b).
Користе се и друге ознаке; у школи најчешће се користи ознака НЗД(a, b).
Примедба 5. Довољно је наћи највећи заједнички делилац за $|a|$ и $|b|$.
Примедба 6. Јасно је да из $c \mid a$ и $c \mid b$ следи $c \mid (a, b)$.
Теорема 6. Ако је d највећи заједнички делилац целих бројева a и b, онда постоје цели бројеви α и β такви да је $\alpha a + \beta b = d$.
Доказ. Посматрајмо скуп целих бројева облика $\alpha a + \beta b$, где су $\alpha, \beta \in \mathbb{Z}$. У том скупу има и позитивних и негативних бројева, а у њему је садржана и нула. Изаберимо у њему најмањи позитиван елемент. Нека је то број $c = \alpha a + \beta b$. Докажимо да $c \mid a$ и $c \mid b$.
Претпоставимо супротно , да c не дели a. Онда постоје такви цели бројеви q и $r, 0 < r < c$, да је $a = cq + r$. Но онда је

$$r = a - cq = a - (\alpha a + \beta b)q = (1 - \alpha q)a - \beta q b,$$

тј. број r је позитиван, мањи од c и линеарна је комбинација бројева a и b, што је супротно претпоставци да је c најмањи такав позитиван број. Дакле, $c \mid a$.
Аналогно се доказује да $c \mid b$, па је број c заједнички делилац бројева a и b, што значи да $\boxed{c \mid d}$.

С друге стране, $c = \alpha a + \beta b$, $d \mid a$ и $d \mid b$ па на основу теореме 3.2° и 1° $\boxed{d \mid c}$. Мора бити $c = d$. □
Дефиниција 5. За целе бројеве a и b кажемо да су **узајамно (релативно) прости** ако је $(a, b) = 1$.
Последица 2. Цели бројеви a и b су узајамно прости акко постоје такви цели бројеви α и β да је $\alpha a + \beta b = 1$.
Теорема 6 нам омогућује и да највећи заједнички делилац бројева a и b окарактеришемо као најмањи позитиван број облика $\alpha a + \beta b, \alpha, \beta \in \mathbb{Z}$.
Дефиниција 6. Највећим заједничким делиоцем целих бројева $a_1, a_2, \dots, a_n$ зовемо највећи од заједничких делиоца ових бројева и обележавамо га са $(a_1, a_2, \dots, a_n)$. Ако је $(a_1, a_2, \dots, a_n) = 1$, бројеви $a_1, a_2, \dots, a_n$ су **узајамно прости**. Бројеви $a_1, a_2, \dots, a_n$ су **узајамно прости по паровима** ако је $(a_i, a_j) = 1$ за свако i, j за које је $1 \le i < j \le n$.

Пример. Бројеви 2,3,4 су узајамно прости јер $(2,3,4) = 1$, али нису узајамно прости по паровима јер $(2,4) = 2$.

Теорема 7. 1° Ако је $a = bq$ и $b > 0$, онда је $(a, b) = b$.

2° $(ma, mb) = m(a, b)$, за $m > 0$.

3° Ако $m \mid a, m \mid b$ и $m > 0$, онда је $\left(\frac{a}{m}, \frac{b}{m}\right) = \frac{1}{m}(a, b)$.

4° Ако је $(a, b) = d$ онда је $\left(\frac{a}{d}, \frac{b}{d}\right) = 1$ (Не мора да важи $\left(\frac{a}{d}, b\right) = 1$).

5° Ако је$(a, m) = (b, m) = 1$, онда је $(ab, m) = 1$.

6° Ако $c \mid ab$ и $(b, c) = 1$, онда је $c \mid a$.

Доказ. 1° Очигледно јер тада

$$(a, b) = (bq, b) = b.$$

2° $m(a, b) = m(\alpha a + \beta b) = \alpha ma + \beta mb = (ma, mb), \alpha, \beta \in \mathbb{Z}$.

3° Ако m дели a и b онда су $\frac{a}{m}$ и $\frac{b}{m}$ цели бројеви. Следи из 2°.

4° $(a, b) = d \Longrightarrow d \mid a$ и $a \mid b$, па су $\frac{a}{d}$ и $\frac{b}{d}$ цели бројеви.

Онда је из 3°

$$\left(\frac{a}{d}, \frac{b}{d}\right) = \frac{1}{d}(a, b) = \frac{1}{d} \cdot d = 1.$$

5° $(a, m) = (b, m) = 1$, па постоје цели бројеви $\alpha_1, \beta_1, \alpha_2, \beta_2$ такви да је

$$\alpha_1 a + \beta_1 m = \alpha_2 b + \beta_2 m = 1.$$

Одавде је, после множења

$$\alpha_1 a \cdot \alpha_2 b = (1 - \beta_1 m)(1 - \beta_2 m) = 1 - mt,\ t = \beta_1 + \beta_2 - \beta_1 \beta_2 m,$$

тј.

$$\alpha_1 \alpha_2 ab + mt = 1,\ \alpha_1 \alpha_2, t \in \mathbb{Z}.$$

Закључујемо да је

$$(ab, m) = 1.$$

6° $(b, c) = 1 \Longrightarrow \alpha b + \beta c = 1, \alpha, \beta \in \mathbb{Z}$. Множећи ову релацију са a добијамо

$$\alpha ba + \beta ca = a.$$

Како $c \mid ab$, то је према теореми 3.2° први сабирак дељив са c.

Како $c \mid c$ према истој теореми и други сабирак је дељив са c.

Па је према теореми 3.1° збир $\alpha ba + \beta ca$ дељив са c, тј. $c \mid a$. □

Теорема 8. Ако је $a = bq + r$, онда је $(a, b) = (b, r)$.

Доказ. Нека је d произвољан заједнички делилац бројева a и b.

Тада из релације $a = bq + r$ следи да је он и делилац броја r $(r = a - bq,$ и теорема 3.1°), тј. заједнички делилац бројева b и r.

Слично, ако је d произвољан заједнички делилац бројева b и r, из исте релације следи да је он и заједнички делилац бројева a и b.

Дакле, скупови заједничких делилаца бројева a и b, односно b и r, поклапају се. Зато су међусобно једнаки и њихови највећи елементи, дакле бројеви (a, b) и (b, r). □

Пример. Одредимо да ли су бројеви 432 и 86 узајамно прости.

Пошто је $432 = 86 \cdot 5 + 2$, то је према теореми $(432,86) = (86,2) = 2$.

Закључујемо да дати бројеви нису узајамно прости.

1.5 Еуклидов алгоритам

Уколико се ради о већим целим бројевима, ефикасан начин налажења највећег заједничког делиоца представља Еуклидов алгоритам. Очигледно је да питање дељивости не зависи од знака, па a и b, можемо сматрати природним бројевима. У складу с раније изложеним можемо исписати следећи низ једнакости (**Еуклидов алгоритам**):

$$\begin{aligned} a &= bq_1 + r_1, & 0 \le r_1 < b, \\ b &= r_1q_2 + r_2, & 0 \le r_2 < r_1, \\ r_1 &= r_2q_3 + r_3, & 0 \le r_3 < r_2, \\ &\dots & \dots \\ r_{n-2} &= r_{n-1}q_n + r_n, & 0 \le r_n < r_{n-1}, \\ r_{n-1} &= r_nq_{n+1}. \end{aligned}$$

Пошто бројеви r_k чине строго опадајући низ природних бројева, то ће се овај низ након коначног броја корака завршити, тј. доћи ћемо до једнакости облика $r_{n-1} = r_nq_{n+1}$.

Теорема 9. Последњи остатак r_n који је различит од нуле у претходном поступку представља највећи заједнички делилац бројева a и b.

Доказ. Користећи теорему 8 лако је констатовати да је задовољен следећи низ једнакости:

$$(a, b) = (b, r_1) = (r_1, r_2) = \dots = (r_{n-2}, r_{n-1}) = (r_{n-1}, r_n).$$

Како је $r_{n-1} = r_nq_{n+1}$, то $r_n \mid r_{n-1}$. Па на основу теореме 7.1°, $(r_{n-1}, r_n) = r_n$, па коначно добијамо да је $(a, b) = r_n$, што је и требало доказати. □

Пример. $a = 936, b = 588.$

$$\begin{aligned} 936 &= 588 \cdot 1 + 384 \\ 588 &= 384 \cdot 1 + 240 \\ 384 &= 240 \cdot 1 + 108 \\ 240 &= 108 \cdot 2 + 24 \\ 108 &= 24 \cdot 4 + 12 \\ 24 &= 12 \cdot 2. \end{aligned}$$

Према томе, $(936{,}588) = 12$. При том је (Враћамо се уназад, изражавамо остатке, редом, како нам наилазе)

$$\begin{aligned} 12 &= 108 - 4 \cdot 24 = 108 - 4(240 - 2 \cdot 108) = 9 \cdot 108 - 4 \cdot 240 \\ &= 9(384 - 240) - 4 \cdot 240 = \\ &= 9 \cdot 384 - 13 \cdot 240 = 9 \cdot 384 - 13(588 - 384) = 22 \cdot 384 - 13 \cdot 588 \\ &= 22(936 - 588) - 13 \cdot 588 = \\ &= 22 \cdot 936 - 35 \cdot 588. \end{aligned}$$

Дакле,

$$12 = 22 \cdot 936 - 35 \cdot 588 \quad \lozenge$$

Примедба 6: У претходном примеру смо показали како се, коришћењем Еуклидовог алгоритма, одређују бројеви α и β такви да је $\alpha a + \beta b = (a, b)$.

Пример. Како је $(13, 60) = 1$, онда према последици 2, можемо записти

$$\boldsymbol{\alpha} \cdot 13 + \beta \cdot 60 = 1.$$

Одредимо бројеве α и β за које ово важи:

$60 = 13 \cdot 4 + 8$, $13 = 8 \cdot 1 + 5$, $8 = 5 \cdot 1 + 3$, $5 = 3 \cdot 1 + 2$, $3 = 2 \cdot 1 + 1$, $2 = 1 \cdot 2$.

Вратимо се уназад

$1 = 3 - 2 = 3 - (5 - 3) = 2 \cdot 3 - 5 = 2(8 - 5) - 5 = 2 \cdot 8 - 3 \cdot 5 = 2 \cdot 8 - 3(13 - 8) =$
$5 \cdot 8 - 3 \cdot 13 = 5(60 - 4 \cdot 13) - 3 \cdot 13 = 5 \cdot 60 - 23 \cdot 13.$

Тражени бројеви су $\alpha = -23, \beta = 5$. $\lozenge$

1.5.1 Визуелизација Еуклидовог алгоритма

Еуклидов алгоритам се може и визуелно приказати коришћењем аналогије са прекривањем правоугаоника квадратима.

Пример. Еуклидов алгоритам за проналажење највећег заједничког делиоца за бројеве 120 и 84:

$$120 = 84 \cdot 1 + 36,$$
$$84 = 36 \cdot 2 + 12,$$
$$36 = 12 \cdot 3,$$

дакле $(120,84) = 12$. Ако желимо да ово визуелно представимо крећемо од правоугаоника димензија 120×84. Он се покрива квадратима странице 84 све док је то могуће, тј. стаје једном. Остаје нам правоугаоник страница 84×36. Он се затим покрива квадратима дужине страница 36, стаје два пута. Као вишак остаје правоугаоник димензија 36×12. Њега је могуће без остатка покрити квадратима чија је страница дужине 12. То значи да је $(120,84) = 12$.

1.5.2 Верижни разломци

Еуклидов алгоритам омогућава да се сваки рационалан број представи у облику коначног верижног разломка.

Коначни верижни разломак је израз облика

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \ddots + \cfrac{1}{a_n}}},$$

где је a_0 цели, а $a_1, a_2, \dots, a_n$ природни бројеви. Јасно је да се сређивањем коначног верижног разломка добија рационалан број. Обратно, сваки рационалан број облика $\frac{a}{b}$ може се записати у облику верижног разломка. Бројеви $a_i, i = \overline{1,n}$ су управо количници који се добијају применом Еуклидовог алгоритма на бројеве a и b:

$$a = ba_0 + r_1,$$
$$b = r_1a_1 + r_2,$$
$$r_1 = r_2a_2 + r_3,$$
$$\dots$$
$$r_{n-1} = r_na_n.$$

Пример. Представити у облику верижног разломка број $\frac{172}{50}$.

$$172 = 50 \cdot 3 + 22,$$
$$50 = 22 \cdot 2 + 6,$$
$$22 = 6 \cdot 3 + 4,$$
$$6 = 4 \cdot 1 + 2,$$
$$4 = 2 \cdot 2,$$

односно, $a_0 = 3, a_1 = 2, a_2 = 3, a_3 = 1, a_4 = 2$, па је

$$\frac{172}{50} = 3 + \cfrac{1}{2 + \cfrac{1}{3 + \cfrac{1}{1 + \frac{1}{2}}}},$$

Односно, верижни облик добијамо на следећи начин:

$$\frac{172}{50} = 3 + \frac{22}{50} = 3 + \frac{1}{\frac{50}{22}} = 3 + \frac{1}{2 + \frac{6}{22}} = 3 + \frac{1}{2 + \frac{1}{\frac{22}{6}}} = 3 + \frac{1}{2 + \frac{1}{3 + \frac{4}{6}}} = \cdots$$

$$= 3 + \frac{1}{2 + \frac{1}{3 + \frac{1}{1 + \frac{1}{2}}}}.$$

Као што је речено, описани поступак развоја важи за рационалне бројеве. Ирационални бројеви одговарају бесконачним верижним разломцима. Примером ћемо илустровати како можемо приближно наћи квадратни корен природног броја.

Пример. Циљ нам је да приближно одредимо $\sqrt{5}$.

Највеће целобројно мање од $\sqrt{5}$ је 2. Тада постоји α, тако да је $\sqrt{5} = \alpha + 2$. За број α важи

$$\alpha = \sqrt{5} - 2 = \frac{\sqrt{5} - 2}{1} \cdot \frac{\sqrt{5} + 2}{\sqrt{5} + 2} = \frac{1}{\sqrt{5} + 2} = \frac{1}{\alpha + 2 + 2} = \frac{1}{\alpha + 4},$$

одатле, примењујући узастопно ове једнакости добијамо бесконачни верижни разломак

$$\sqrt{5} = \alpha + 2 = 2 + \frac{1}{4 + \alpha} = \cdots = 2 + \frac{1}{4 + \frac{1}{4 + \frac{1}{\ddots}}}.$$

За коначан број чланова овог развоја добијамо приближну вредност броја $\sqrt{5}$. Тако је

$$\sqrt{5} \approx 2 + \frac{1}{4} = 2.25,$$

$$\sqrt{5} \approx 2 + \frac{1}{4 + \frac{1}{4}} = 2.235,$$

$$\sqrt{5} \approx 2 + \frac{1}{4 + \frac{1}{4 + \frac{1}{4}}} = 2.2361. \qquad \Diamond$$

1.6 Најмањи заједнички садржалац

Дефиниција 7. Садржалац датог броја a јесте сваки цео број који је дељив бројем a. Скуп свих садржалаца броја a означавамо са S_a.

Дефиниција 8. Цео број s је **заједнички садржалац** бројева a и b ако $a \mid s$ и $b \mid s$.

Скуп свих садржалаца нема највећи елемент, али дефинишемо:

Дефиниција 9. Најмањи међу позитивним заједничким садржаоцима бројева a и b зове се **најмањи заједнички садржалац** тих бројева и обележава се са $[a, b]$.

Јасно је да је $[a, b] = [-a, b] = [a, -b] = [-a, -b]$.

Као и код највећег заједничког делиоца, од других могућих ознака поменимо НЗС(a, b).

Дефиниција 10. Заједничким садржаоцем целих бројева $a_1, a_2, \ldots, a_n$, називамо сваки број који је дељив сваким од бројева $a_1, a_2, \ldots, a_n$. Најмањи позитиван међу њима зове се најмањи заједнички садржалац ,и обележава се са $[a_1, a_2, \ldots, a_n]$.

Очито важи следеће тврђење.

Теорема 10. 1° Ако је $s = [a_1, a_2, \dots, a_n]$ и S ма који заједнички садржалац бројева $a_1, a_2, \dots, a_n$, онда $s \mid S$, што значи да су сви заједнички садржаоци бројева $a_1, a_2, \dots, a_n$ облика $S = sq, q \in \mathbb{Z}$.

2° Ако $b_1 \mid b, b_2 \mid b, \dots, b_n \mid b$, онда $[b_1, b_2, \dots, b_n] \mid b$.

Теорема 11.

1° $(a, b)[a, b] = |a, b|$.

2° Ако је $(a, b) = 1$, онда је $[a, b] = |ab|$.

3° Ако је $m \in \mathbb{N}$, онда је $[ma, mb] = m[a, b]$.

Доказ.

1° Пошто прелаз са скупа природних бројева на скуп целих бројева не представља тешкоћу, докажимо теорему за природне бројеве.

Нека је S ма који заједнички садржалац бројева a и b. Онда је

$$a \mid S \Longrightarrow S = ak.$$

Пошто и $b \mid S \Longrightarrow \frac{S}{b} = \frac{ak}{b}$ мора бити цео број. $(*)$

Нека је $d = (a, b)$, онда $d \mid a$ и $d \mid b$, па одатле

$$a = \alpha d \text{ и } b = \beta d, \text{где су } (\alpha, \beta) = 1. \qquad (**)$$

Из $(*)$ и $(**)$ добијамо

$$\frac{ak}{b} = \frac{\alpha dk}{\beta d} = \frac{\alpha k}{\beta} \in \mathbb{Z},$$

а пошто је $(\alpha, \beta) = 1$ то мора бити $k = \beta t, t \in \mathbb{N}$.

Према томе

$$S = ak = a\beta t = a \cdot \underbrace{\frac{b}{d}}_{b=\beta d} \cdot t = \frac{ab}{d} t, t \in \mathbb{N}.$$

С друге стране, сваки број облика $\frac{ab}{d} t$ је садржалац бројева a и b. Дакле, број S је заједнички садржалац бројева a и b акко је

$$S = \frac{ab}{d} t, t \in \mathbb{N}.$$

Најмањи такав број добијамо за $t = 1$, односно $s = \frac{ab}{d}$, тј. $[a, b] = \frac{ab}{(a,b)}$.

2° Следи из 1°.

3° Из 1° имамо да је

$$[ma, mb] = \frac{|mamb|}{(ma,mb)} \overset{\text{T.7.2°}}{=} \frac{m^2|ab|}{m(a,b)} = m\frac{|ab|}{(a,b)} = m[a, b]. \qquad \square$$

1.7 Услов за дељивост неким природним бројем

Критеријуми дељивости нам служе за испитивање да ли је да ли је дати број дељив са фиксним делиоцем, али без извођења поступка дељења већ, најчешће, испитујући цифре датог броја.
За исти број постоје различити критеријуми дељивости и овде ћемо дати правила која се често користе у основној школи, као и доказе који су примерени да се раде у узрасту петог разреда.
Касније ћемо видети друге начине за доказивање, који су подеснији за средњу школу.

1.7.1. Критеријуми дељивости:

- Број је дељив декадном јединицом ако на крају има бар онолико нула колико има та декадна јединица.
- Број је дељив са 2 ако је последња цифра тог броја дељива са 2 (ако је 0,2,4,6 или 8);
- Број је дељив са 5 ако је последња цифра тог броја дељив са 5 (ако је 0 или 5);
- Број је дељив са 4 ако му је двоцифрени завршетак дељив са 4;
- Број је дељив са 8 ако му је троцифрени завршетак дељив са 8;
- Број је дељив са 25 ако му је двоцифрени завршетак дељив са 25.
- Број је дељив са 3 ако му је збир цифара дељив са 3.
- Број је дељив са 9 ако му је збир цифара дељив са 9.
- Број је дељив са 11 ако је разлика броја десетица и цифре јединица дељива са 11. (Број је дељив са 11 ако му је разлика збира цифара на непарним и парним местима, дељива са 11.)
- Број је дељив са 7 ако је разлика броја десетица и двоструке цифре јединица дељива са 7.

За последња два правила, поступак се понавља све док се не дође до броја за који смо сигурни је ли дељив или није поменутим бројем.
Доказ. На примерима конкретних бројева су изложене идеје доказа ових тврђења, јер на тај начин се подстиче и развија логичко размишљање.

1) **Критеријуми за бројеве који су делиоци неких декадних јединица**

Дељивост бројевима 2 и 5:
Последња цифра неког броја је остатак при дељењу тог броја са 10. На пример, 1765=176·10+5 Како је први сабирак дељив са 2 и са 5 то дељивост броја 1765 са 2 и са 5 зависи само од другог сабирка, односно од цифре јединица.
Дељивост бројевима 4 и 25:
Двоцифрени завршетак неког броја одређује остатак при дељењу тог броја са 100. На пример, 3 236=32·100 + 36. Како је 100 = 4·25, то значи да је први сабирак дељив 4 и са 25 и дељивост броја 3236 са 4 и са 25 зависи само од другог сабирка, односно двоцифреног завршетка броја.

2) **Критеријуми за бројеве који не деле ниједну декадну јединицу**

Дељивост бројевима 3 и 9:
Пре свега истакнимо да сви бројеви који су за 1 мањи од деканде јединице дељиви су са 9.
Пример. 9 999 = 9 · 1 111, 999 = 9 · 111, итд. Како је један од чинилаца дељив са 9 па је према теореми 3.2° производ дељив са 9, а самим тим и са 3, јер 9=3·3.

Дати природни број раставимо на цифру јединица, десетица, стотина…па искористимо претходно речено. На пример,

$$4\,563=4\cdot 1\,000 + 5\cdot 100 + 6\cdot 10 + 3=4\cdot(999+1) + 5\cdot(99+1) + 6\cdot(9+1) + 3 =$$
$$= 4\cdot 999 + 4 + 5\cdot 99 + 5 + 6\cdot 9 + 6 + 3 = \underline{4\cdot 999 + 5\cdot 99 + 6\cdot 9} + 4 + 5 + 6 + 3.$$

Како су прва три сабирка дељива са 9 (сваки је записан у облику производа два број од којих је један дељив са 9), закључујемо да дељивост броја зависи само од збира 4+5+6+3= 18, што представља збир цифара датог броја. Како $9 \mid 18$, то и $9 \mid 4563$.
Слично се испитује и дељивост са 3, искористимо дати пример

$$4\,563=\underline{4\cdot 999 + 5\cdot 99 + 6\cdot 9} + 4 + 5 + 6 + 3.$$

Дакле, прва три сабирка из примера су дељива са 9, а самим тим и са 3, па дељивост са 3 зависи само од збира цифара тог броја.

Дељивост бројевима 7 и 11:
Доказаћемо правило дељивости бројем 7, дељивост са бројем 11 се аналогно доказује.
Нека је: d – број десетица датог броја b, j – његова цифра јединица. Тада је број b облика

$$b = 10d + j.$$

Претпоставимо да је разлика броја десетица броја b и двоструке цифре јединица $2j$ дељива са 7. То значи да је

$$d - 2j = 7k, j \in \{0,1,\dots,9\}, k \in \mathbb{Z}, d \in \mathbb{N}.$$

Покажимо да је и број b дељив са 7.

$$b = 10d + j = 10(7k + 2j) + j = 70k + 20j + j = 70k + 21j.$$

Како су оба сабирка дељива са 7, то је и збир дељив са 7.
***Задатак* 2.** Доказати:

1) Број је дељив с 13 ако је збир броја десетица и 4-струке цифре јединица дељив с 13.
2) Број је дељив с 37 ако је разлика броја десетица и 11-струке цифре јединица дељива с 37.

Решење. Доказујемо као у случају дељивости са 7. ◊
Приметимо да важи, остататак при дељењу броја са 3 (9) је једнак остатку при дељењу суме цифара тог броја са 3 (9). Остатак при дељењу броја са 2 (5) је једнак остатку при дељењу једноцифреног завршетка тог броја са 2 (5). Остатак при дељењу броја са 4 (25) је једнак остатку при дељењу двоцифреног завршетка тог броја са 4 (25).

1.7.2. Дељивост сложеним бројевима

Помоћу поменутих критеријума дељивости показујемо дељивост осталих бројева.
Дељивост са 6
Ако је природан број n дељив и са 2 и са 3, онда је он дељив и са 6.
Доказ. Ако је природан број n дељив и са 2 и са 3, онда се он може написати као $n = 2k$ и $n = 3l$, где су k и l такође природни бројеви. Одатле следи да је $2k = 3l$, то јест $k = \frac{3l}{2}$.
Пошто је k природан број, мора бити природан број и $\frac{3l}{2}$. Пошто 3 није дељиво са 2, мора l бити дељиво са 2, те га можемо писати као
$l = 2m$, где је m природан број.
На почетку смо имали $n = 3l$, сада то можемо писати као $n = 3l = 3\cdot 2m = 6m$. Овим је доказано да је n дељив са 6.
Наравно, ако је број дељив са 6 онда је он дељив са свим његовим делиоцима, тј, дељив је бројевима 2 и 3.
Дељивост са 18
Скуп делилаца броја 18 јесте $D_{18} = \{1,2,3,6,9,18\}$, односно број 18 можемо записати

$$18 = 1 \cdot 18 = 2 \cdot 9 = 3 \cdot 6.$$

Поставља се питање како одабрати одговарајућу комбинацију бројева. Ако је број дељив са 18 онда је он дељив свим његовим делиоцима, и то ћемо искористити.

Погледајмо комбинацију $18 = 2 \cdot 9$; доказали бисмо дељивост бројевима 2 и 9; ако је број дељив са 9 онда је он дељив и са 3 па смо показали дељивост и са 3; ако је број дељив и са 2 и са 3, онда је он дељив и са 6. Дакле, показали смо дељивост тог броја са свим делиоцима броја 18.

Погледајмо комбинацију $18 = 3 \cdot 6$; доказали бисмо дељивост бројевима 3 и 6, односно бројевима 3 и 2. Ако је број дељив са 3 то не значи да је дељив и са 9, па је јасно да овом комбинацијом нећемо „покупити″ све делиоце броја 18.

Закључујемо, број је дељив са 18 ако је дељив са 2 и 9.

Заправо, ово можемо доказати аналогно као у случају дељивости бројем 6.

2 ПРОСТИ БРОЈЕВИ

Ученицима петог разреда задаци из ових области јесу занимљиви, али доста греше. Утисак је да још увек не умеју да се изразе и да прате ток својих мисли, тј. да владају свим идејама. Тек касније, у седмом и осмом разреду, схвате и разумеју проблематику из ове овласти.

Дефиниција 1. Цео број $p > 1$ је **прост** ако је дељив само јединицом и самим собом**.** Цео број $m > 1$ је **сложен** ако није прост. Број 1 није ни прост ни сложен.
Пример.

- Првих неколико простих бројева: $2, 3, 5, 7, 11, 13, 17, 19, \ldots$
- Првих неколико сложених бројева: $4, 6, 8, 9, 10, 12, 14, 15, 16, 18, 20, \ldots$

Приметимо:

1) Најмањи делилац, већи од јединице, произвољног целог броја већег од 1, јесте прост број. Заиста, нека је $a > 1$ и q његов најмањи делилац који је већи од 1. Ако би број q био сложен, он би имао неки делилац p за који би важило $1 < p < q$. Но, тада би p био делилац и броја a, па q не би био најмањи међу делиоцима броја a који су већи од 1.
2) Једина два узастопна проста броја су 2 и 3. Ово следи из чињенице да је 2 једини паран прост број, а то следи из тога што је сваки паран број већи од 2 дељив са 2, па је сложен.

Теорема 1. (Еуклид) Постоји бесконачно много простих бројева. Другим речима, од сваког простог броја постоји већи прост број.
Доказ. Претпоставимо да тврђење теореме није истинито, тј. да постоји коначно много простих бројева $p_1, p_2, \ldots, p_k$, а да су сви остали природни бројеви већи од 1 сложени. Број

$$N = p_1 p_2 \cdots p_k + 1$$

Је према томе сложен. Но, онда он мора бити дељив неким од простих бројева, што је немогуће јер N при дељењу било којим од бројева $p_1, p_2, \ldots, p_k$ даје остатак 1. Тиме смо доказали да је тврђење теореме истинито. □

Теорема 2. Ако је дат произвољан природан број n, увек се може наћи n узастопних сложених бројева.
Доказ. Број $n!$ је дељив са првих n природних бројева. Ако му, на пример, додамо број 4 добијамо нови сложен број $n! + 4$ који је дељив са 4. Нама је потребан низ узастопних сложених бројева, стога посматрајмо бројеве

$$A_1 = (n+1)n(n-1)\cdots 3 \cdot 2 \cdot 1 + 2 \rightarrow \text{дељив бројем 2},$$
$$A_2 = (n+1)n(n-1)\cdots 3 \cdot 2 \cdot 1 + 3 \rightarrow \text{дељив бројем 3},$$
$$\cdots$$
$$A_n = (n+1)n(n-1)\cdots 3 \cdot 2 \cdot 1 + (n+1) \rightarrow \text{дељив бројем n} + 1.$$

То су узастопни природни бројеви, има их тачно n и сви су сложени. □

Да бисмо генерисали све просте бројеве мање од датог природног броја N, можемо се послужити такозваним **Ератостеновим ситом (решетом)**:
1° Исписујемо све природне бројеве до N,

$$\sout{1}, 2, 3, 4, 5, \sout{6}, 7, \sout{8}, 9, \sout{10}, 11, \sout{12}, 13, \sout{14}, 15, \sout{16}, 17, \ldots, N$$

2° Најпре прецртамо јединицу;
3° Први прост број је 2, њега остављамо а прецртамо све бројеве дељиве са 2 (они су сложени);
4° Прецртамо све бројеве веће од 3 и дељиве са 3;
5° Следећи непрецртани број је 5. Он је прост, јер да није већ би био прецртан. Прецртамо све бројеве веће од 5 и дељиве са 5;
⋮
Понављајући овај поступак јасно је да смо елиминисали све сложене бројеве и да смо издвојили просте бројеве мање од N. У сваком кораку, први непрекрижени број је прост, па у наредном кораку крижамо његове садржаоце. Први прекрижени број ће бити његов квадрат, јер су сви мањи садржаоци већ прекрижени (Рецимо код броја 5, већ су прекрижени бројеви 10, 15, 20, први који крижамо је 25). Фибоначи је приметио да је довољно елиминисати сложене бројеве, који су садржаоци простих бројева мањих од $\sqrt{N}$.

Теорема 3. Позитиван цео број N је сложен ако и само ако има прост фактор p, такав да је $p \leq \sqrt{N}$.
Доказ. Ако N има прост фактор $p \leq \sqrt{N}$, тада је N, очигледно сложен број.
Обратно, нека је N сложен број и p његов најмањи прост фактор. Тада је $N = pm$, где је m цео број и $m \geq p$. Тада је

$$N = m \cdot p \geq p \cdot p = p^2,$$

следи да је

$$\sqrt{N} \geq p. \quad \square$$

Пример. Ако хоћемо да испишемо просте бројеве од 1 до 100, треба елиминисати сложене бројеве дељиве, редом, са 2,3,5 и 7, јер је $\sqrt{100} = 10$ и најмањи прост број мањи од 10 је 7.
На тај начин добијамо 25 простих бројева мањих од 100:
$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97.$ ◊
Пример.

- Хоћемо да испитамо да ли је број 119 прост. Треба испитати да ли је дељив простим бројевима мањим од $\sqrt{119}$. Како је $10^2 < 119 < 11^2$, треба испитати дељивост простим бројевима мањим од 11 а то су бројеви 2, 3, 5 и 7. Непосредном провером откривамо да је 119 сложен број, тј. важи једнакост $119 = 7 \cdot 17$.
- Слично, посматрајмо број 1999. Како је $44^2 < 1999 < 45^2$ треба испитати дељивост броја 1999 простим бројевима мањим од 45,
  а то су бројеви 2, 3, 5 , 7, 11, 13, 17, 19, 23, 29, 31, 37, 41 и 43. Како није дељив ниједним од њих, закључујемо да је он прост.

Поменућемо још један критеријум за испитивање да ли је неки број прост, који припада Леонарду Ојлеру.
Теорема 4. (Ојлеров критеријум) Ако непаран природан број $n, n > 1$, може да се представи у виду разлике квадрата два природна броја на више од једног начина, он је сложен. Ако је то представљање јединствено, он је прост. $\square$

Приметимо да за сваки непаран број $n, n > 1$ важи разлагање

$$n = \left(\frac{n+1}{2}\right)^2 - \left(\frac{n-1}{2}\right)^2,$$

Па приликом испитивања да ли је прост треба потражити да ли поред овог разлагања постоји још једно. За примену овог критеријума могу да се користе таблице квадрата природних бројева. Ако испитујемо да ли је дати број $n, n > 1$ прост или није, узастопно му додајемо квадрате природних бројева r, са особином $r < \frac{n-1}{2}$.

Ако је за неко r, $n + r^2$ потпун квадрат, број је сложен јер из $r^2 + n = a^2$, следи да је $n = a^2 - r^2$.

Пример.

- Посматрајмо број 31. Додајемо му редом квадрате $1^2, 2^2, 3^2, \dots, r^2, r < 15$. Ниједан од бројева $31 + r^2$ није потпун квадрат те је број 31 прост.
- Посматрајмо број 3551. Из таблице квадрата додајемо му редом квадрате $1^2, 2^2, 3^2, \dots, r^2, r < 1775$. Како је $3551 + 7^2 = 60^2$, број 3551 је сложен. Наиме, разлагање $3551 = 60^2 - 7^2$ се разликује од разлагања

  $$3551 = \left(\frac{3551+1}{2}\right)^2 - \left(\frac{3551-1}{2}\right)^2 = 1776^2 - 1775^2.$$

Теорема 5. Ако је p прост број и $p \mid ab$, онда $p \mid a$ или $p \mid b$.

Доказ. Претпоставимо да $p \nmid a$. Онда су p и a узајамно прости бројеви. Али онда, према теореми 1.7.6°, $p \mid b$. □

Општије:

Теорема 6. Ако је p прост број и $p \mid a_1 a_2 \cdots a_k$, тада дели барем један од бројева $a_1, a_2, \dots, a_k$.

Доказ. Доказати помоћу математичке индукције и претходне теореме. □

***Задатак* 1:** Сваки прост број p већи од 3 има облик $6k + 1$ или $6k - 1$. Докажи.

Решење. Скуп целих бројева можемо поделити на шест класа бројева, према остатку при дељењу са 6[2]. То су бројеви облика $6k, 6k + 1, 6k + 2, 6k + 3, 6k + 4, 6k + 5$ (остатак при дељењу са 6 може бити 0,1,2,3,4 или 5).

Бројеви облика $6k, 6k + 2, 6k + 3, 6k + 4$ су сложени јер су дељиви неким од бројева 2 или 3. Дакле сви прости бројеви припадају класама бројева облика $6k + 1$ или $6k + 5$.

Још важи (Поглавље три, недостатак), $6k + 5$ је исто што и $6k - 1$. ◊

***Задатак* 2.** Сваки прост број p већи од 2 има облик $4k + 1$ или $4k - 1$. Докажи.

Решење. Аналогно као у претходном задатку. ◊

***Задатак* 3.** Прости бројеви 3, 5 и 7 су једина тројка узастопних непарних простих бројева.

Решење. Дакле, тражимо тројке узастопних простих непарних бројева. Са p означимо најмањи од тих бројева, тада су $p, p + 2, p + 4$ узастопни непарни бројеви. Треба да покажемо да су они прости.

Ако је $p = 3$, онда је $p + 2 = 5$ и $p + 4 = 7$. То је наша тројка.

Нека је $p > 3$, онда је p облика $6k + 1$ или $6k - 1$.

Ако је $p = 6k + 1$, онда је $p + 2 = 6k + 1 + 2 = 6k + 3$, а то је сложен број јер је дељив са 3.

Ако је $p = 6k - 1$, онда је $p + 4 = 6k - 1 + 4 = 6к + 3$, а то је сложен број јер је дељив са 3.

Закључујемо да је тројка 3, 5 и 7 једина таква тројка бројева. ◊

---

[2] Поглавље три, класе конгуенције.

Теорема 7. (Основни став аритметике) Сваки природан број N већи од 1 може се једнозначно изразити у облику производа простих чинилаца:

$$N = p_1 p_2 \cdots p_k, \;\; p_i \text{ прост}, i = \overline{1,k}.$$

Доказ. Доказаћемо математичком индукцијом.

Ако је N прост број, тврђење очигледно важи.

Претпоставимо да тврђење важи за сваки сложен број мањи од N. Докажимо да тврђење важи и за N.

Ако је N сложен број, тада постоји цео број, већи од 1 а мањи од N, који дели N. Најмањи такав означимо са p_1. Број p_1 не може бити сложен, јер би у том случају постојао цео број k, такав да $1 < k < p_1$ и $k \mid p_1$, што повлачи да број k дели N и да је мањи од p_1. То је, међутим, у контрадикцији да је p_1 најмањи такав број. Дакле p_1 је прост број.

Следи да је $N = p_1 N_1, 1 < N_1 < N$. По претпоставци индукције број N_1 се може представити у облику простих фактора, према томе, онда може и N.

Јединственост репрезентације:

Претпоставимо да исти број има две репрезентације, рецимо

$$N = p_1 p_2 \cdots p_k = q_1 q_2 \cdots q_l,$$

где су p_i и q_j прости бројеви. Узмимо произвољан прост чинилац прве репрезентације, рецимо p_i. Пошто производ $q_1 q_2 \cdots q_l$ мора бити дељив простим бројем p_i, онда на основу теореме 5 један од његових чинилаца мора бити дељив са p_i. Но, како су $q_1, q_2, \ldots, q_l$ прости бројеви, то мора постојати $q_j = p_i$. Аналогно, за свако q_j постоји неко $p_i = q_j$. □

Пример. $120 = 2 \cdot 2 \cdot 2 \cdot 3 \cdot 5.$

Ако се у разлагању броја N неки чиниоци понављају, па се, рецимо, p_1 јавља α_1 пута, p_2 јавља α_2 пута,…, $p_к$ јавља $\alpha_к$ пута, онда се облик

$$N = {p_1}^{\alpha_1} {p_2}^{\alpha_2} \cdots {p_k}^{\alpha_k}$$

зове канонски облик природног броја N (**канонска факторизација**).

Пример. $120 = 2^3 \cdot 3 \cdot 5.$

Помоћу канонске факторизације датих бројева a и b лако се одређује њихов највећи заједнички делилац и најмањи заједнички садржалац. Наиме, ако је

$$a = {p_1}^{\alpha_1} {p_2}^{\alpha_2} \cdots {p_k}^{\alpha_k}, \qquad b = {p_1}^{\beta_1} {p_2}^{\beta_2} \cdots {p_k}^{\beta_k},$$

неки од бројева α_i, β_i могу бити и једнаки нули (ако се неки број не појављује као чинилац), тада:

$$(a,b) = {p_1}^{min\{\alpha_1,\beta_1\}} {p_2}^{min\{\alpha_2,\beta_2\}} \ldots {p_k}^{min\{\alpha_k,\beta_k\}},$$
$$[a,b] = {p_1}^{max\{\alpha_1,\beta_1\}} {p_2}^{max\{\alpha_2,\beta_2\}} \ldots {p_k}^{max\{\alpha_k,\beta_k\}}.$$

Пример. $120 = 2^3 \cdot 3 \cdot 5$ и $84 = 2^2 \cdot 3 \cdot 7$, тј.

$120 = 2^3 \cdot 3 \cdot 5 \cdot 7^0$ и $84 = 2^2 \cdot 3 \cdot 5^0 \cdot 7$, па је

$$(120,84) = 2^2 \cdot 3 \cdot 5^0 \cdot 7^0 = 2^2 \cdot 3 = 12,$$

једноставније речено, узимамо само онолико колико се појављује у оба броја.

$$[120,84] = 2^3 \cdot 3 \cdot 5 \cdot 7 = 840.$$

Теорема 8. Природан **број је квадрат** онда и само онда ако у канонској факторизацији има све изложиоце парне.

Доказ. Нека је канонска репрезентација природног броја $n = {p_1}^{\alpha_1} {p_2}^{\alpha_2} \cdots {p_k}^{\alpha_k}$.

Нека је $n = m^2, m = {q_1}^{\beta_1} {q_2}^{\beta_2} \cdots {q_l}^{\beta_l}$ канонска репрезентација броја m. Тада је

$$n = {p_1}^{\alpha_1} {p_2}^{\alpha_2} \cdots {p_k}^{\alpha_k} = \left({q_1}^{\beta_1} {q_2}^{\beta_2} \cdots {q_l}^{\beta_l}\right)^2 = {q_1}^{2\beta_1} {q_2}^{2\beta_2} \cdots {q_l}^{2\beta_l}.$$

Како је канонска факторизација датог броја јединствена, то у овом случају мора бити

$$k = l, p_i = q_i \text{ и } \boxed{\alpha_i = 2\beta_i}, \text{ за свако } 1 \le i \le k \ (k = l).$$

Обратно, претпоставимо да број r у својој канонској репрезентацији има за изложиоце парне бројеве, тј. $n = {p_1}^{2\alpha_1}{p_2}^{2\alpha_2}\cdots{p_k}^{2\alpha_k}$. Тада

$$n = {p_1}^{2\alpha_1}{p_2}^{2\alpha_2}\cdots{p_k}^{2\alpha_k} = ({p_1}^{\alpha_1}{p_2}^{\alpha_2}\cdots{p_k}^{\alpha_k})^2 = m^2 \text{ за } m = {p_1}^{\alpha_1}{p_2}^{\alpha_2}\cdots{p_k}^{\alpha_k}. \quad \square$$

Пример. $17424 = 2^4 \cdot 3^2 \cdot 11^2 = (2^2 \cdot 3 \cdot 11)^2 = 132^2$.

Теорема 9. Ако је производ два узајамно проста природна броја квадрат целог броја,

$$ab = c^2, \qquad (a, b) = 1,$$

тада су a и b квадрати целих бројева: $a = {a_1}^2, b = {b_1}^2$.

Доказ. Да би број био квадрат , према претходној теореми, неопходно је и довољно да су му сви експоненти у факторизацији парни (c^2 има парне експоненте). Како су a и b узајамно прости, сваки прост делилац броја c^2 јавља се или у a или у b, али не у оба; зато прости фактори бројева a и b морају имати парне експоненте. $\square$

***Задатак* 4**. Квадрат сваког простог броја p, ако је $p > 3$, има облик $12n + 1$. Докажи.

Решење. Сваки прост број $p > 3$ је облика $6k \pm 1$. Одатле је

$$p^2 = (6k - 1)^2 = 36k - 12k + 1 = 12(3k - 1) + 1.$$

Аналогно за $p = 6k + 1$. $\lozenge$

Теорема 10. Нека је $a = {p_1}^{\alpha_1}{p_2}^{\alpha_2}\cdots{p_k}^{\alpha_k}$ канонска факторизација броја a. Тада су сви **позитивни делиоци** броја a облика

$$d = {p_1}^{\beta_1}{p_2}^{\beta_2}\cdots{p_k}^{\beta_k}, \quad 0 \le \beta_1 \le \alpha_1, 0 \le \beta_2 \le \alpha_2, \ldots, 0 \le \beta_k \le \alpha_k.$$

Доказ. Следи на основу тога што је $a = d \cdot n$, где је $d = {p_1}^{\delta_1}{p_2}^{\delta_2}\cdots{p_k}^{\delta_k}$ и $\delta_i = \alpha_i - \beta_i$. $\square$

Пример. $120 = 2^3 \cdot 3 \cdot 5$, па су позитивни делиоци броја 120 облика

$$2^i \cdot 3^j \cdot 5^k, 0 \le i \le 3, 0 \le j \le 1, 0 \le k \le 1,$$

тј. бројеви

$2^0 \cdot 3^0 \cdot 5^0 = \mathbf{1}$	$2^0 \cdot 3^0 \cdot 5^1 = \mathbf{5}$	$2^0 \cdot 3^1 \cdot 5^0 = \mathbf{3}$	$2^1 \cdot 3^0 \cdot 5^0 = \mathbf{2}$
$2^2 \cdot 3^0 \cdot 5^0 = \mathbf{4}$	$2^3 \cdot 3^0 \cdot 5^0 = \mathbf{8}$	$2^0 \cdot 3^1 \cdot 5^1 = \mathbf{15}$	$2^1 \cdot 3^1 \cdot 5^1 = \mathbf{30}$
$2^2 \cdot 3^1 \cdot 5^1 = \mathbf{60}$	$2^3 \cdot 3^1 \cdot 5^1 = \mathbf{120}$	$2^1 \cdot 3^0 \cdot 5^1 = \mathbf{10}$	$2^2 \cdot 3^0 \cdot 5^1 = \mathbf{20}$
$2^3 \cdot 3^0 \cdot 5^1 = \mathbf{40}$	$2^1 \cdot 3^1 \cdot 5^0 = \mathbf{6}$	$2^2 \cdot 3^1 \cdot 5^0 = \mathbf{12}$	$2^3 \cdot 3^1 \cdot 5^0 = \mathbf{24}$

Дакле, број 120 има 16 позитивних делилаца. $\lozenge$

Специјално,

Сваки делилац броја a је на јединствен начин одређен избором експонента β_i.

Како β_i можемо да изаберемо на $\alpha_i + 1$ начина, то је укупан број позитивних делилаца броја a (укључујући 1 и само a) једнак

$$(\alpha_1 + 1)(\alpha_2 + 1)\cdots(\alpha_k + 1).$$

Последњи израз има посебну ознаку, дефинишемо:

Дефиниција 2. Укупан **број позитивних делилаца** природног броја a означавамо са $\boldsymbol{\tau(a)}$. Дакле,

$$\tau(a) = (\alpha_1 + 1)(\alpha_2 + 1)\cdots(\alpha_k + 1)$$

ако је $a = {p_1}^{\alpha_1}{p_2}^{\alpha_2}\cdots{p_k}^{\alpha_k}$ његова канонска факторизација.

Пример. $120 = 2^3 \cdot 3 \cdot 5$, па је $\tau(120) = (3 + 1)(1 + 1)(1 + 1) = 16$.

У следећој табели дато је неколико првих вредности функције τ.

n	1	2	3	4	5	6	7	8	9	10	11	12
$\tau(n)$	1	2	2	3	2	4	2	4	3	4	2	6

Јасно је да:

1) Ако је a прост број $\tau(a) = 2$.
2) Ако a има само један прост делилац, тј. канонска факторизација броја a је облика $a = p^{\alpha}$, тада $\tau(a) = \alpha + 1$.

Пример. $9 = 3^2 \Longrightarrow \tau(9) = 2 + 1 = 3$, заиста позитивни делиоци броја 9 су бројеви 1,3, 9.

3) Ако је канонска факторизација броја a облика $a = p_1 p_2 \cdots p_k$, тада $\tau(a) = \underbrace{(1+1)(1+1)\cdots(1+1)}_{k \text{ пута}} = 2^k$.

Пример. $30 = 2 \cdot 3 \cdot 5 \Longrightarrow \tau(15) = 2^3 = 8$, заиста позитивни делиоци броја 30 јесу бројеви 1,2,3,5,6,10,15,30.

***Задатак* 5.** Ако природан број n има непаран број различитих позитивних делилаца, он је потпун квадрат. Доказати.

Решење. Ако је $n = {p_1}^{\alpha_1} {p_2}^{\alpha_2} \cdots {p_k}^{\alpha_k}$ и $\tau(n) = (\alpha_1 + 1)(\alpha_2 + 1)\cdots(\alpha_k + 1)$ непаран број, онда сви $\alpha_i + 1$ морају бити непарни, тј. бројеви α_iморају бити парни, што значи да је n потпун квадрат. ◊

Дефиниција 3. Функција $f: \mathbb{N} \longrightarrow \mathbb{Z}$ за коју важи

1) За неко $n \in \mathbb{N}$ је $f(n) \neq 0$,
2) $f(mn) = f(m)f(n)$ за све m, n такве да је $(m, n) = 1$, зовемо **мултипликативна функција**.

Теорема 11. Функција τ је мултипликативна.

Доказ. 1) Важи, је за свако $n \in \mathbb{N}$ је $\tau(n) \neq 0$,

2) Ако су бројеви m и n узајамно прости, тада је

$$m = {p_1}^{\alpha_1} {p_2}^{\alpha_2} \cdots {p_k}^{\alpha_k}, n = {q_1}^{\beta_1} {q_2}^{\beta_2} \cdots {q_l}^{\beta_l},$$

при чему се ниједан од бројева p_i не поклапа ни са једним од бројева q_j. Зато је

$$mn = {p_1}^{\alpha_1} {p_2}^{\alpha_2} \cdots {p_k}^{\alpha_k} {q_1}^{\beta_1} {q_2}^{\beta_2} \cdots {q_l}^{\beta_l}$$

канонска факторизација броја mn, па је

$$\tau(mn) = (\alpha_1 + 1)\cdots(\alpha_k + 1)(\beta_1 + 1)\cdots(\beta_l + 1) = \tau(m)\tau(n). \quad \square$$

Пример. $\tau(24) = \tau(2^3 \cdot 3) = \tau(2^3)\tau(3) = (3 + 1)(1 + 1) = 8$.

Поред броја позитивних делилаца датог броја a посматрајмо и њихов збир.

Дефиниција 4. Збир свих позитивних делилаца природног броја a означава се са $\boldsymbol{\sigma(a)}$.

Јасно је да:

1) Ако је a прост број, онда је $\sigma(a) = a + 1$, јер прост број a има само та два делиоца.
2) Ако је $a = p^{\alpha}, p$ прост број, онда је $\sigma(a) = 1 + p + p^2 + \cdots + p^{\alpha} \underbrace{=}_{\substack{\text{геометријски} \\ \text{низ}}} \frac{p^{\alpha+1}-1}{p-1}$,

Пример. $27 = 3^3$, па је $\tau(27) = 4$ и то су бројеви $1, 3, 3^2, 3^3$. Дакле, $\sigma(27) = \sigma(3^3) = 1 + 3 + 3^2 + 3^3$.

Теорема 12. Нека је $a = {p_1}^{\alpha_1} {p_2}^{\alpha_2} \cdots {p_k}^{\alpha_k}$ канонска факторизација природног броја a, онда је

$$\sigma(a) = \frac{{p_1}^{\alpha_1+1} - 1}{p_1 - 1} \cdot \frac{{p_2}^{\alpha_2+1} - 1}{p_2 - 1} \cdots \frac{{p_k}^{\alpha_k+1} - 1}{p_k - 1}.$$

Доказ. Вредност $\sigma(a)$ можемо записати у облику

$$\sigma(a) = \sum_{\substack{d \mid a \\ d > o}} d.$$

Како је, према теореми 10, сваки такав делилац облика $d = {p_1}^{\beta_1}{p_2}^{\beta_2}\cdots{p_k}^{\beta_k},\ 0 \le \beta_i \le \alpha_i,\ 1 \le i \le k,$ то је

$$\sigma(a) = \sum_{\substack{0\le\beta_i\le\alpha_i \\ 1\le i\le k}} {p_1}^{\beta_1}{p_2}^{\beta_2}\cdots{p_k}^{\beta_k}$$

$$= (1 + p_1 + \cdots + {p_1}^{\alpha_1})(1 + p_2 + \cdots + {p_2}^{\alpha_2})\cdots(1 + p_k + \cdots + {p_k}^{\alpha_k}).$$

Наиме, множећи изразе последњег производа добијамо управо сабирке који се појављују у претходно наведеној суми. Сабирањем геометријских низова у заградама, долазимо до израза датог у формулацији теореме. □

Наведимо неколико вредности функције σ.

n	1	2	3	4	5	6	7	8	9	10	11	12
$\sigma(n)$	1	3	4	7	6	12	8	15	13	18	12	28

Теорема 13. Функција σ је мултипликативна.
Доказ. Слично као доказ теореме 11. □
Пример. $\sigma(120) = \sigma(2^3 \cdot 3 \cdot 5) = \frac{2^4-1}{2-1} \cdot \frac{3^2-1}{3-1} \cdot \frac{5^2-1}{5-1} = 360.$

Примедба 1. У скупу $\mathbb{Z}$ бројеви -1 и 1 нису ни прости ни сложени. То су такозвани јединични елементи – елементи који деле сваки цео елемент. Прости елементи у $\mathbb{Z}$ су бројеви $\pm2, \pm3, \pm5$ ...
Дефиниција 5. Елемент a је еквивалентан елементу b ако је $a = -1 \cdot b, a, b \in \mathbb{Z}$.
Пример. Елементи 2 и -2 су еквивалентни; 3 и -3 су еквивалентни…
Дефиниција 6. За елемент, који није 0 и није јединични, кажемо да је прост ако нема других делилаца осим јединичних и себи еквивалентног елемента.
Пример. Из претходно реченог следи да су бројеви $\pm2, \pm3, \pm5$ ... прости у $\mathbb{Z}$.
Примедба 2. Из овог произилази и јединственост факторизације у $\mathbb{Z}$:

$$6 = 2 \cdot 3 = (-2)(-3),$$

а како су прости чиниоци -2 и -3 еквивалентни бројевима 2 и 3, редом, та два растављања су иста до на редослед и еквивалентност чинилаца.

2.1 Врсте простих бројева

Пријатељски бројеви – два броја за које важи да је збир позитивних делилаца било ког од та два броја, не рачунајући тај број, једнак оном другом:
Пример:

- За број 220 то су бројеви: $1, 2, 4, 5, 10, 11, 20, 22, 44, 55, 110$ и њихов збир је 284.
  За број 284 то су бројеви: $1, 2, 4, 71, 142$ и њихов збир је 220.

Дакле, 220 и 284 су пријатељски бројеви.

- За број 6 то су бројеви: $1, 2, 3$ и њихов збир је 6.

Дакле, број 6 је сам себи пријатељ и њега називамо савршени број. ◊
Савршени број – број који је једнак збиру својих позитивних делилаца, не рачунајући сам тај број (Сам свој пријатељ).
Пример: бројеви 6, 28, 496, 8128…
Алгоритам за налажење парних савршених бројева дао је још Еуклид:
Рачунамо суме $1 + 2 + 4 + 8 + \cdots$, ако је збир прост број, помножимо га са последњим сабирком и добијамо савршен број.

$$1+2=\mathbf{3}\rightarrow 3\cdot 2=\mathbf{6}$$
$$1+2+4=\mathbf{7}\rightarrow 7\cdot 4=\mathbf{28}$$
$$1+2+4+8+16=\mathbf{31}\rightarrow 31\cdot 16=\mathbf{496}$$
$$1+2+4+8+16+32+64=\mathbf{127}\rightarrow 127\cdot 64=\mathbf{8128.}\quad \Diamond$$

Сви данас познати савршени бројеви су парни и облика $(2^n-1)2^{n-1}$, при чему је 2^n-1 прост Марсенов број (Што је Еуклид и тврдио).

Дефиниција 7. Бројеви облика 2^n-1 зову се **Марсенови бројеви**.

Теорема 14. Ако је 2^n-1 прост број, онда је и n прост број:

Доказ. Претпоставимо супротно, да је n сложен број, тј. $n=ab,\ 1<a,b<n$. Тада би број

$$2^n-1=2^{ab}-1=(2^a)^b-1^b$$

био дељив са 2^a-1. □

Марсенови прости бројеви су:

$$2^2-1=\mathbf{3}$$
$$2^3-1=\mathbf{7}$$
$$2^5-1=\mathbf{31}$$
$$2^7-1=\mathbf{127}$$
$$\dots$$
$$n\in\{2,3,5,7,13,17,19,31,61,89,107,\dots\}$$

Видимо да сваком савршеном броју одговара један Марсенов прост број.

Као што је познати савршени бројеви су парни и не зна се постоји ли иједан непаран савршен број.

Факторијални прости бројеви - прости бројеви облика $n!\pm 1, n\in\mathbb{N}$:

2, 3, 5, 7, 23, 719, 5 039, 39 916 801, 479 001 599, 87 178 291 199...

Палиндромни прости бројеви - прости бројеви који се исто читају и са лева на десно и са десна на лево:

2, 3, 5, 7, 11, 101, 131, 151, 181, 191, 313, 353, 373, 383, 727, 757, 787, 797, 919, 929, 10 301, 10 501…

Емирп - прост број који читан здесна на лево опет даје прост број:

13, 17, 31, 37, 71, 73, 79, 97, 107, 113…

Питагорејски прости бројеви

5, 13, 17, 29, 37, 41, 53, 61, 73, 89, 97, 101, 109, 113, 137, 149, 157, 173, 181, 193, 197, 229, 233, 241, 257, 269, 277, 281, 293, 313, 317, 337, 349, 353, 373, 389, 397, 401, 409, 421, 433, 449, 457, 461

Прости бројеви састављени само од јединица - бројеви састављени од 2, 19,23, 317, 1031 јединица су прости бројеви.

Прости бројеви близанци - парови простих бројева који се разликују за два:

(3, 5), (5, 7), (11, 13), (17, 19), (29, 31), (41, 43), (59, 61), (71, 73), (101, 103), (107, 109), (137, 139)...

3 КОНГРУЕНЦИЈЕ БРОЈЕВА

Ова тема не обрађује се у склопу редовне наставе у основној школи, али ни у средњој школи јој се не посвећује пуно пажње. У основној школи обрађује се на додатној настави, у оквиру припрема за такмичење. Када заврше основно и средње образовање, ученици, углавном, познају само појам конгруентности и неке њене основне особине.

3.1 Дефиниција релације конгруенције

Релацију конгруенције представио је и развио немачки математичар Карл Фридрих Гаус у свом делу „Питања о аритметици″ (Disquisitiones arithmeticae, 1801.). Гаус се фокусирао на остатак који се добије када се један природан број дели с другим природним бројем; тај остатак се обично не узима у разматрање мада се у вези њега може навести читав низ занимљивих особина бројева.

Будући да је број a дељив бројем b ако и само ако је дељив са $-b$, без умањења општости усредсредићемо се на скуп природних бројева.

Дефиниција 1. Нека је дат природан број m, већи од 1. Два су цела броја a и b конгруетна по модулу m ако дају исти остатак при дељењу са m. Пишемо:

$$a \equiv b \ (mod \ m).$$

Ако a и b не дају исти остатак при дељењу са m, каже се да a није конгуентно b по модулу m и пише се

$$a \not\equiv b \ (mod\, m).$$

Пример.

- $26 \equiv 41 \ (mod\ 5)$ јер при дељењу са 5 оба броја дају остатак 1.
- $8 \not\equiv 4 (mod\ 3)$ јер при дељењу са 3 дају различите остатке.

Примедба 1: $26 \equiv 41 \ (mod\ 5)$ можемо записати и као $26 \equiv_5 41$.

Теорема 1. Нека је *m* природан број, *a, b, r* цели бројеви. Тада важи:

1° $a \equiv b \ (mod \ m)$ ако и само ако је разлика бројева a и b дељива са m.

$$\boxed{\boldsymbol{a \equiv b \ (mod \ m) \Leftrightarrow m \mid a - b}}$$

2° $a \equiv b \ (mod \ m)$ ако и само ако је $a = b + mt$ за неки цео број t.

$$\boxed{\boldsymbol{a \equiv b \ (mod \ m) \Leftrightarrow a = b + mt}}$$

3° *r* је остатак при дељењу *a* са *m* ако и само ако је $a \equiv r \ (mod\, m)$, тј. сваки цели број a је конгруентан са својим остатком r по модулу m.

$$\boxed{\underbrace{\boldsymbol{a = mq + r}}_{\text{Т.о дељењу са остатком}} \quad \Leftrightarrow \boldsymbol{a \equiv r \ (mod \ m)}}$$

Доказ.

1° Нека важи $a \equiv b \ (mod \ m) \overset{\text{деф.1.}}{\Longrightarrow} a{:}\, m = q_1(\boldsymbol{r}),\ b{:}\, m = g_2(\boldsymbol{r}) \implies a = mq_1 + \boldsymbol{r},\ b = mq_2 + \boldsymbol{r}$.

Када одузмемо $a - b = mq_1 - mq_2 = m(q_1 - q_2)$.

Како је $m(q_1 - q_2)$ дељиво са m то је и разлика $a - b$ дељива са m.

Обратно, нека важи $m \mid a - b$, покажимо да a и b дају исти остатак при дељењу са m.

$$m \mid a - b \Rightarrow a - b = mq \qquad (1)$$

Нека је $a = mq_1 + r_1$ и $b = mq_2 + r_2$. Тада

$$a - b = m(q_1 - q_2) + (r_1 - r_2) \qquad (2)$$

Из (1) и (2) следи да је

$$mq = m(q_1 - q_2) + (r_1 - r_2)$$

Тј. $r_1 - r_2 = 0 \Longrightarrow r_1 = r_2$, што значи a и b да дају једнаке остатке при дељењу са m

$$a \equiv b \ (mod \ m).$$

2° Показаћемо да важи помоћу претходног тврђења.

$$a \equiv b \ (mod \ m) \Longrightarrow m \mid a - b \Longrightarrow a - b = mq \Longrightarrow a = b + mg, g \coloneqq t$$

Обратно, $a = b + mt \Longrightarrow a - b = mt \Longrightarrow m \mid a - b \overset{1°}{\Rightarrow} a \equiv b \ (mod \ m)$.

3° r је остатак при дељењу a са m, значи да можемо записати $a = mq + r, 0 \leq r < m$.

$$a = mq + r \overset{2°}{\Leftrightarrow} a \equiv r \ (mod \ m) \quad \square$$

Пример.

- $17 \equiv -9 \ (mod \ 13)$ јер је $13 \mid 17 - (-9)$.
- $23 \equiv 2 (mod \ 7)$ јер је 2 остатак при дељењу 23 са 7.

Примедба 2. $23 \equiv 2 (mod \ 7)$ можемо записати и као $23 (mod \ 7) = 2$.

Нека је s број који са бројем a даје збир дељив са m, тј. нека је $m \mid a + s$, односно $m \mid a - (-s)$. Можемо закључити да је :

$$\boxed{\boldsymbol{a \equiv -s (mod \ m)}}$$

Ако је уз то $0 \leq s < |a|$, тада можемо рећи да је s **недостатак** при дељењу a броја са бројем m. Према томе, број a је конгруентан по модулу m своме остатку и своме „минус недостатку".

Пример. $120 \equiv 10 (mod \ 11)$ али и $120 \equiv -1 (mod \ 11)$ јер броју 120 недостаје још 1 да би се без остатка могло извршити дељење са 11.

Приметимо, збир остатака и недостатака дају модуо m.

Пример. Ако делимо са 17 и недостатак је 4, то значи да је остатак 13.

3.2 Особине релације конгруенције

Теорема 2. Бити конгруентан по датом модулу је релација еквиваленције у скупу целих бројева.

1) $a \equiv a \ (mod \ m)$ (рефлексивност)
2) $a \equiv b \ (mod \ m)$, онда $b \equiv a \ (mod \ m)$ (симетричност)
3) $a \equiv b \ (mod \ m)$ и $b \equiv c \ (mod \ m)$, онда $a \equiv c \ (mod \ m)$ (транзитивност)

Доказ.

1) $a \equiv a \ (mod \ m) \Longrightarrow m \mid a - a,$ тј. $m \mid 0$.
2) $a \equiv b \ (mod \ m) \Longrightarrow m \mid a - b$; $a - b = -(b - a)$, па из овога имамо $m \mid -(b - a)$, а одатле $m \mid b - a \Longrightarrow b \equiv a \ (mod \ m)$
3) $a \equiv b \ (mod \ m) \Longrightarrow m \mid a - b$
   $b \equiv c \ (mod \ m) \Longrightarrow m \mid b - c$
   следи
   $m \mid (a - b) + (b - c)$
   $m \mid a - c$
   Тј. $a \equiv c \ (mod \ m)$ $\square$

Пример.

- $22 \equiv 15 (mod \ 7) \Leftrightarrow 15 \equiv 22 (mod \ 7)$,
- $22 \equiv 15 (mod \ 7)$ и $15 \equiv 29 (mod \ 7)$, онда је $22 \equiv 29 (mod \ 7)$.

Још нека од основних својстава конгруенције дата су у следећој теореми.

Теорема 3. Нека су a, b, c, d цели бројеви.

1° Ако је $a \equiv b \ (mod \ m)$ и $c \equiv d \ (mod \ m)$ онда је $ac \equiv bd \ (mod \ m)$, $a + c \equiv b + d \ (mod \ m)$ и $a - c \equiv b - d \ (mod \ m)$.

2° Ако је $a \equiv b \ (mod \ m)$ и $c \equiv d \ (mod \ m)$ онда је $ax + cy \equiv bx + dy \ (mod \ m)$ за свака два цела броја x, y.

3° Ако је $a \equiv b \ (mod \ m)$, онда је $ac \equiv bc \ (mod \ m)$, а такође и $ac \equiv bc \ (mod \ mc)$ за сваки $c \neq 0$.

4° Ако је $a \equiv b \ (mod \ m)$ и $d \mid m$, онда је $a \equiv b \ (mod \ d)$.

Доказ. У доказу користимо $a \equiv b \ (mod \ m) \Leftrightarrow m \mid a - b$, тј. $a - b = mt$.

1° Важи $a - b = mt, c - d = mt_1$.

Потребно је показати да из тога следи да :

$$m \mid ac - bd, \qquad m \mid (a + c) - (b + d), \qquad m \mid (a - c) - (b - d)$$

- $ac - bd = (b + mt)(d + mt_1) - bd = bd + mtd + mt_1 b + m^2 tt_1 - bd = m(td + t_1 b + tt_1)$.

Дакле, важи $m \mid ac - bd$.

- $(a + c) - (b + d) = \underline{a - b} + \underline{c - d} = mt + mt_1 = m(t + t_1)$.
- $(a - c) - (b - d) = a - b - c + d = a - b - (c - d) = m(t - t_1)$.

2° Важи $a - b = mt, c - d = mt_1$.

Потребно је показати да важи : $m \mid ax + cy - bx + dy$.

$$ax + cy - bx + dy = x(a - b) + y(c + d) = xmt + ymt_1 = m(xt + yt_1).$$

3° Важи $a - b = mt$.

$$ac - bc = c(a - b) = \boldsymbol{cm}t$$

4° Важи $a - b = mt$ и из $d \mid m \Longrightarrow m = dt_1$.

$$a - b = mt = dt_1 t \Longrightarrow d \mid a - b. \quad \square$$

Задатак 1. *Докажи* $a \equiv b \ (mod \ m) \Leftrightarrow a - b \equiv 0 \ (mod \ m)$.

Решење. $a \equiv b \ (mod \ m) \Leftrightarrow m \mid a - b$, тј. остатак при дељењу броја $a - b$ бројем m јесте 0, а према теореми сваки број је конгруентан свом остатку. ◊

Следеће теореме су уопштења неких наведених тврђења.

Теорема 4. Ако су $a_1, a_2, \dots, a_n, \ b_1, b_2, \dots, b_n$ и $m \neq 0$ цели бројеви тада из релације

$$a_1 \equiv b_1, a_2 \equiv b_2, \dots, a_n \equiv b_n \ (mod \ m)$$

следи

$$a_1 + a_2 + \cdots + a_n \equiv b_1 + b_2 + \cdots + b_n \ (mod \ m)$$

Доказ. У доказу ове теореме користићемо теорему 3.1° и принцип математичке индукције.

Тврђење је тачно за $n = 2$ јер на основу поменуте теореме имамо:

$$a_1 \equiv b_1 (mod \ m) \text{ и } a_2 \equiv b_2 \ (mod \ m) \Longrightarrow a_1 + a_2 \equiv b_1 + b_2 \ (mod \ m)$$

Нека је тврђење тачно за $n - 1$, докажимо да важи и за n:

Важи

$$a_1 \equiv b_1, a_2 \equiv b_2, \dots, a_{n-1} \equiv b_{n-1} \ (mod \ m) \Longrightarrow$$
$$a_1 + a_2 + \cdots + a_{n-1} \equiv b_1 + b_2 + \cdots + b_{n-1} \ (mod \ m).$$

Ако је поред тога $a_n \equiv b_n \ (mod \ m)$, из претходног имамо

$$(a_1 + a_2 + \cdots + a_{n-1}) + a_n \equiv (b_1 + b_2 + \cdots + b_{n-1}) + b_n \ (mod \ m). \quad \square$$

Теорема 5. . Ако су $a_1, a_2, \dots, a_n,\ b_1, b_2, \dots, b_n$ и $m \neq 0$ цели бројеви тада из релације

$$a_1 \equiv b_1, a_2 \equiv b_2, \dots, a_n \equiv b_n \ (mod\ m)$$

следи

$$a_1 a_2 \dots a_n \equiv b_1 b_2 \dots b_n \ (mod\ m).$$

Доказ. Као и у претходном доказу користимо математичку индукцију и теорему 3.1°. □

Последица 1. Ако су a, b и $m \neq 0$ цели бројеви тада из релације $a \equiv b\ (mod\ m)$ следи

$$a^n \equiv b^n (mod\ \ m),$$

где је $n \in \mathbb{N}_0$.

Доказ. Следи непосредно из теореме 5.

$$a^n = \underbrace{aa \dots a}_{n \text{ пута}}, a = a_1 = \dots = a_n$$

$$b^n = \underbrace{bb \dots b}_{n \text{ пута}}, b = b_1 = \dots = b_n. \quad \square$$

Задатак 2. Користећи претходна тврђења одреди остатак који се добија дељењем броја 3^{100} бројем 13.

Решење. Идеја је да нађемо број са што мањим остатком при дељењу са 13.

Како је $3 \equiv 3\ \ (mod\ 13),\ \ 3^2 \equiv 9\ (mod\ 13), 3^3 \equiv 27 \equiv 1\ (mod\ 13)$.

Дакле,

$$3^3 \equiv 1\ (mod\ 13) \Longrightarrow (3^3)^{33} \equiv 1^{33}\ (mod\ 13),$$

$$3^{99} \equiv 1\ (mod\ 13).$$

Односно, $3 \equiv 3\ \ (mod\ 13)$ и још $3^{99} \equiv 1\ (mod\ 13)$, па имамо:

$$3^{100} = 3 \cdot 3^{99} = 3 \cdot (3^3)^{33} \equiv 3 \cdot 1^{33} \equiv 3 \cdot 1 \equiv 3(mod\ 13)$$

Закључујемо да је 3 остатак при дељењу 3^{100} са 13 (важи $0 \leq 3 < 13$, што мора важити за остатак). ◊

Задатак 3. Колики је остатак дељења $1 \cdot 2 \cdot 3 \cdot \dots \cdot 9 \cdot 10$ са 11?

Решење: Олакшаћемо рачун користећи остатак 1 и недостатак -1.

$$1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot 7 \cdot 8 \cdot 9 \cdot 10 = 1 \cdot 2 \cdot 5 \cdot 3 \cdot 4 \cdot 10 \cdot 6 \cdot 7 \cdot 8 \cdot 9$$

$$= 1 \cdot 10 \cdot 12 \cdot 10 \cdot 6 \cdot 7 \cdot 8 \cdot 9$$

Из овога имамо:

$$1 \cdot 2 \cdot 3 \cdot \dots \cdot 9 \cdot 10 \equiv 1 \cdot (-1) \cdot 1 \cdot (-1) \cdot 6 \cdot 7 \cdot 8 \cdot 9 \equiv 1 \cdot (-1)^2 \cdot (-5) \cdot (-4) \cdot (-3) \cdot (-2)$$

$$\equiv$$

$$\equiv 1 \cdot 1 \cdot (-1)^4 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \equiv 5 \cdot 2 \cdot 4 \cdot 3 \equiv (-1) \cdot 12 \equiv (-1) \cdot 1 \equiv -1(mod\ 11).$$

Недостатак при дељењу датог броја са 11 износи -1, па је остатак при дељењу датог броја са 11 једнак 10. ◊

Из овог примера видимо како нам коришћење недостатака некад може олакшати рачун.

Теорема 6. Ако је $a \equiv b\ (mod\ m)$ и ако $c \mid a$ и $c \mid b$, тада је

$$\frac{a}{c} \equiv \frac{b}{c}\ \left(mod\ \frac{m}{d}\right), \text{где је } d = (c, m). \qquad (1)$$

Доказ. Потребно је показати

$$\frac{m}{d} \mid \frac{a}{c} - \frac{b}{c}.$$

Имамо следеће податке:

$$a \equiv b\ (mod\ m) \Longrightarrow m \mid a - b$$

$$d = (c, m) \Longrightarrow d \mid c \text{ и } d \mid m \text{ и } \left(\frac{c}{d}, \frac{m}{d}\right) = 1$$

$$c \mid a \text{ и } c \mid b \Longrightarrow c \mid a - b$$

Одатле

$$\left.\begin{matrix} d \mid m \\ m \mid a-b \end{matrix}\right\} \Rightarrow d \mid a-b$$

$$\left.\begin{matrix} m \mid a-b \\ d \mid m \\ d \mid a-b \end{matrix}\right\} \Rightarrow \frac{m}{d} \mid \frac{a-b}{d}$$

Дакле

$$\frac{m}{d} \mid \frac{a-b}{d}$$
$$\frac{m}{d} \mid \frac{a-b}{d} \cdot \frac{c}{c}$$
$$\boxed{\frac{m}{d} \mid \frac{a-b}{c} \cdot \frac{c}{d}}$$

Међутим, због $\left(\frac{c}{d}, \frac{m}{d}\right) = 1$ из последњег мора бити

$$\frac{m}{d} \mid \frac{a-b}{c}. \quad \square$$

Специјално,

1° Ако $(\boldsymbol{c}, \boldsymbol{m}) = \boldsymbol{1} = \boldsymbol{d}$, заменом у (1) добијамо да важи $\frac{a}{c} \equiv \frac{b}{c} \ (mod\ m)$.

2° Ако $\boldsymbol{c} \mid \boldsymbol{m} \Longrightarrow (\boldsymbol{c}, \boldsymbol{m}) = \boldsymbol{c}$, па заменом у (1) добијамо да важи $\frac{a}{c} \equiv \frac{b}{c} \left(mod\ \frac{m}{c}\right)$.

Из претходног се види да се скраћивање код конгруенције не може увек извести.

Пример.

- $42 \equiv 84\ (mod\ 6), 7 \mid 42, 7 \mid 84, (7,6) = 1 \Longrightarrow 6 \equiv 12\ \ (mod\ 6)$.
- $42 \equiv 84\ (mod\ 6), 14 \mid 42, 14 \mid 84$, а ми урадимо следеће $3 \equiv 6\ \ (mod\ 6)$ добијамо нетачан резултат. Јер $(14,6) = 2$, па је тачно $3 \equiv 6\ \ (mod\ 3)$.

Теорема 7. Скуп свих целих бројева x конгруетних са a по модулу m дат је изразом

$$x = a + tm, t = 0, \pm 1, \pm 2, \ldots$$

Доказ. Бројеви x конгруетни са a по модулу $m \longrightarrow a \equiv x\ (mod\ m) \overset{\text{T.2.2}}{\Longleftrightarrow} x \equiv a (mod\ m) \overset{\text{T.1.2°}}{\Longleftrightarrow} x = a + mt.$ $\square$

3.3 Системи остатака, класе конгруенције, потпун и сведен систем

Ако цео број делимо са 2, може се десити или да буде дељив (ми га онда зовемо парним) или да даје остатак 1 (тада га зовемо непарним). На тај начин, сви су цели бројеви разложени на две дисјунктне класе бројева, на парне и непарне бројеве.

Сви цели бројеви који дају исти остатак при дељењу са датим бројем (конгруентни су по датом модулу) образују једну **класу бројева.**

Пример. По модулу 3 остаци могу бити $0,1,2$, тако да имамо три класе бројева:

1° класу бројева облика $3k$ који су дељиви са три, односно конгруентни су нули по модулу 3.

$$[0] = (\ldots, -6, -3, 0, 3, 6, \ldots)$$

2° класу бројева облика $3k + 1$ који приликом дељења са 3 дају остатак 1, односно конгруетни су јединици по модулу 3.

$$[1] = (\ldots, -5, -2, 1, 4, 7, \ldots)$$

3° класу бројева облика $3k+2$ који приликом дељења са 3 дају остатак два, односно конгруетни су двојци по модулу 3.

$$[2] = (\dots, -4, -1, 2, 5, 8, \dots)$$

Овим смо скуп целих бројева поделили на три класе. Ако се неки број налази у класи $[0]$ (тј. остатак је 0 при дељењу са 3) он се неће налазити ни у једној другој класи (не може имати два различита остатка) и још важи да сваки број из скупа $\mathbb{Z}$ мора припадати некој од ових класа јер мора давати неки од ова три остатка. Односно поделили смо скуп $\mathbb{Z}$ на три дисјунктне класе бројева. ◊

Нека је дат природан број $m > 1$; остаци при дељењу са m могу бити: $0,1,2,\dots,(m-1)$; посматрајмо класе целих бројева конгруентне редом бројевима : $0,1,2,\dots,(m-1)$ по модулу m. Очигледно је да су тим класама исцрпљени сви цели бројеви и да, уз то, нема пресецања између класа, односно један број не може бити у две различите класе. На тај начин извршено је разлагање скупа $\mathbb{Z}$ на m класа, а бројеви $0,1,2,\dots,(m-1)$ карактеришу класу бројева у којој се налазе, па их можемо изабрати да представљају класу којој припадају. За представника класе, заправо, можемо изабрати било који елемент из те класе, сви они дају исти остатак.

Пример. У претходном примеру, бројеви $0,1,2$ карактеришу класу (говоре колики је остатак при дељењу са 3) и њих можемо узети за представнике, али исто тако можемо узети нпр. за представника класе $[1]$ било који елемент те класе, рецимо број 7. ◊

Скуп тако изабраних представника зовемо **потпуним системом остатака** по модулу m. Како представнике можемо да изаберемо на различите начине то значи да и систем можемо изабрати на различите начине. Важно је да изабраних m бројева буду сваки из по једне класе (Тада је сваки цели број конгруентан по модулу m са тачно једним од њих).

Остатке $0,1,2,\dots,(m-1)$ називамо **најмањи ненегативни остаци** па добијени систем називамо **систем најмањих ненегативних остатака.**

Ако се из потпуног система остатака одстране бројеви који нису узајамно прости са m добијамо такозвани **сведени (редуковани) систем остатака** по датом модулу m.

Пример . Ако посматрамо остатке по модулу 8, тада бројеви $0,1,2,3,4,5,6,7$ чине потпуни, а $1,3,5,7$ редуковани систем остатака по модулу 8.

Сваки цео број је конгруентан по модулу 8 неком од бројева из потпуног система остатака по модулу 8.

Сваки број узајамно прост са 8 је конгруентан по модулу 8 неком од бројева из редукованог система остатака по модулу 8. ◊

Уопштимо последња два тврђења из примера:

1° Нека је $(a, m) = 1$ и нека је $\{\alpha_1, \alpha_2, \dots, \alpha_k\}$ редукован систем остатака по модулу m. Тада је a конгруентан по модулу m неком од бројева из датог редукованог система.

Доказ. Нека је $a \equiv r(mod\ m), 0 \le r < m$ (увек важи).

Онда из $a = mq + r, 0 \le r < m$, следи да је $(a, m) = \boxed{(m, r) = 1}$, Значи да r припада редукованом систему по модулу m и a му је конгруентан по модулу m □

2° У сведеном систему остатака по датом модулу m увек ће бити исти број елемената, без обзира од ког потпуног система да пођемо.

Доказ. Нека је $\{0,1,2,\dots,(m-1)\}$ потпун систем најмањих ненегативних остатака по модулу m.

Изаберимо друге представнике класа и нека они образују следећи потпуни систем остатака по модулу m: $\{\alpha_0, \alpha_1, \dots, \alpha_{m-1}\}$.

Елемент α_i припада редукованом систему по модулу m ако и само ако је $(\alpha_i, m) = 1$.

Знамо $\alpha_i \in \{\alpha_0, \alpha_1, \dots, \alpha_{m-1}\}$ је представник класе бројева који дају остатак $r_i \in \{0,1,2, \dots, (m-1)\}$. То значи

$$\alpha_i \equiv r_i (mod\ m), 0 \leq r_i < m,$$
$$\alpha_i = mq + r_i, 0 \leq r_i < m.$$

Одавде, према теореми 1.8, имамо

$$(\alpha_i, m) = (m, r_i)$$

tj,

$$(\alpha_i, m) = 1 \iff (m, r_i) = 1, \text{ за } i \in \overline{0, m-1}.$$

То значи да ће редуковани системи имати једнак број елемената. □

Теорема 8. Нека је $(\alpha, m) = 1$ и нека је $\{\alpha_1, \alpha_2, \dots, \alpha_k\}$ произвољан потпун (сведен) систем остатака по модулу m. Тада је $\{\alpha\alpha_1, \alpha\alpha_2, \dots, \alpha\alpha_k\}$ исто тако потпун (сведен) систем остатака по модулу m.

Доказ.

У оба система има једнак број елемената.

Потребно је показати да ако је $i \neq j$ онда бројеви $\alpha\alpha_i$ и $\alpha\alpha_j$ припадају различитим класама,тј. $\alpha\alpha_i \not\equiv \alpha\alpha_j\ (mod\ m)$ ако $i \neq j$.

Претпоставимо супротно, $\alpha\alpha_i \equiv \alpha\alpha_j\ (mod\ m)$. Тада према теореми 6, због $(\alpha, m) = 1$, важи да је

$$\frac{\alpha\alpha_i}{\alpha} \equiv \frac{\alpha\alpha_j}{\alpha} \left(mod\ \frac{m}{1}\right),$$
$$\alpha_i \equiv \alpha_j (mod\ m),$$

што је немогуће.

$\{\alpha\alpha_1, \alpha\alpha_2, \dots, \alpha\alpha_k\}$ је сведени систем остатака по модулу m: ако се ради о сведеном систему остатака, тј. ако је $(\alpha_i, m) = 1$ за $i = \overline{1,k}$, онда је и $(\alpha\alpha_i, m) = 1$ за $i = \overline{1,k}$ $((\alpha, m) = 1)$ па скуп $\{\alpha\alpha_1, \alpha\alpha_2, \dots, \alpha\alpha_k\}$ представља сведени систем остатака по модулу m. □

Пример. Ако поново посматрамо остатке по модулу 8: $\{0,1,2,3,4,5,6,7\}$ потпуни, а $\{1,3,5,7\}$ редуковани систем остатака по модулу 8. Како је $(8,11) = 1$ то је $\{0,11,22,33,44,55,66,77\}$ потпуни, а $\{11,33,55,77\}$ редуковани систем остатака по модулу 8.

Задатак 4. Доказати да је збир квадрата два цела броја дељив са 7 само ако су оба броја дељива са 7.

Решење. Нека су a и b цели бројеви. Треба доказати $7 \mid a^2 + b^2$ ако $(7 \mid a^2 \wedge 7 \mid b^2)$.

Скуп целих бројева може се поделити на 7 класа конгруенције по модулу 7. Према последици 1, ако квадрате ових бројева поделимо са 7 остаци могу бити $0, 1,2,4$.

Јер, ако је број c представник класе бројева који су конгруентни броју 3 по модулу 7, из последице 1 имамо $c \equiv 3(mod 7) \Rightarrow c^2 \equiv 3^2 \equiv 2(mod\ 7)$, и тако за сваки остатак:

остатак: $0,1,2,3,4,5,6$

квадрат:0,1,4,9,16,25,36

конгруентан:0,1,4,2,2,4,1

Збир било која два од ових остатака не може бити 7 ни 0, сем када су оба остатка 0, а то је остатак при дељењу са 7 квадрата бројева из класе бројева облика $7k$, тј. бројева дељивих са 7. ◊

3.4 Ојлерова теорема, Фермаова теорема

Дефиниција 2. Број природних бројева који нису већи од датог произвољног броја m и узајамно су прости са њим, тј. број елемената произвољног сведеног система остатака по модулу m означава се са $\varphi(m)$. Функција φ зове се **Ојлерова функција**.

Неколико првих вредности функције φ дато је следећом таблицом.

m	1	2	3	4	5	6	7	8	9	10	11	12
$\varphi(m)$	1	1	2	2	4	2	6	4	6	4	10	4

Како су за **прост број p** сви елементи скупа $\{1,2,\dots,p\}$, сем p, узајамно прости са p, то је $\boldsymbol{\varphi(p) = p - 1}$.
Ако је $\boldsymbol{m = 2^k}$, лако се проверава (из наредног тврђења следи, 2 је прост број) да је $\boldsymbol{\varphi(m) = 2^{k-1}}$.

Теорема 9. Ако су n и p природни бројеви и p прост број, тада је

$$\varphi(p^n) = p^{n-1}(p-1) = p^n\left(1 - \tfrac{1}{p}\right).$$

Доказ. Занима нас колико има природних бројева мањих од p^n и узајамно простих са p^n. Сваки од природних бројева од 1 до p^n или је дељив са p или је узајамно прост са p. Број оних који су дељиви са p (самим тим дељиви су и са p^n) једнак је $p^n : p = p^{n-1}$. Остаје да је број оних који су узајамно прости са p (према томе и са p^n) једнак

$p^n - p^{n-1} = p^n\left(1 - \frac{1}{p}\right)$. □

Задатак 5. Колико има бројева који су узајамно прости са бројем 14 641 и који нису већи од њега?
Решење: $14\,641 = 11^4 \Longrightarrow p = 11, n = 4 \Longrightarrow \varphi(11^4) = 11^3 \cdot 10 = 13310$. ◊

Дефиниција 3. Функција $f: \mathbb{N} \longrightarrow \mathbb{Z}$ за коју важи

3) За неко $n \in \mathbb{N}$ је $f(n) \neq 0$,
4) $f(mn) = f(m)f(n)$ за све m, n такве да је $(m,n) = 1$, зовемо **мултипликативна функција**.

Теорема 10. Ојлерова функција φ је мултипликативна($\varphi(mn) = \varphi(m)\varphi(n)$).
Доказ.

1) $\varphi(2) = 1$
2) Нека је $(m,n) = 1$; треба одредити $\varphi(mn)$, односно број елемената који су узајамно прости са mn. Знамо да је број узајамно прост са производом mn ако и само ако је узајамно прост са m и са n. Бројеве $1,2,\dots,mn$ запишимо у облику табеле:

$\boldsymbol{1}$	2	$\dots$	k	$\dots$	$\boldsymbol{n}$
$n+1$	$n+2$	$\dots$	$n+k$	$\dots$	$2n$
$\dots\dots\dots\dots\dots$	$\dots\dots$	$\dots$	$\dots\dots\dots\dots\dots\dots\dots\dots$	$\dots$	$\dots\dots\dots$
$(m-1)n+1$	$(m-1)n+2$	$\dots$	$(m-1)n+k$	$\dots$	$\boldsymbol{mn}$

Узајамно простих са n: у k −тој колони сви бројеви имају облик $in + k$, $i = \overline{0, m-1}$, сви су они конгруентни по модулу n, тј. сви су они узајамно прости са n ако и само ако је k узајамно прост са n. Дакле, у било којој колони дате табеле или су сви елементи узајамно прости са n или ниједан.

У првом реду табеле $(1,2,\dots,k,\dots,n)$ има $\varphi(n)$ бројева који су узајамно прости са n, што значи да у табели има $\varphi(n)$ колона у којима су сви елементи узајамно прости са n.
Сада ћемо да утврдимо колико у свакој таквој колони има бројева који су узајамно прости са m: посматрајмо поново бројеве у k −тој колони (претпоставимо да су узајамно прости са n). Међу њима не постоје два конгруентна по модулу m (који припадају истој класи). Ако би постојали

$$sn + k \equiv tn + k\ (mod\ m), 0 \le s < t \le m - 1$$

тада је

$$sn \equiv tn(mod\ m)$$

А како је $(m, n) = 1$, то је према теореми 6

$$s \equiv t(mod\ m).$$

Бројеви s и t припадају потпуном систему остатака по модулу m $(0 \le s < t \le m - 1)$, па из последње конгруенције следи да мора бити $s = t$, што је контрадикција.
Дакле, у k −тој колони налази се m бројева и сваки од њих припада различитој класи по модулу m, што значи да они образују потпун систем остатака по модулу m. Одатле имамо да је број елемената узајамно простих са m једнак $\varphi(m)$.
Коначно, у свакој од $\varphi(n)$ колона које садрже бројеве узајамно просте са n, има тачно $\varphi(m)$ бројева узајмно простих са m. Тиме је доказано да је $\varphi(mn) = \varphi(m)\varphi(n)$. □
Теорема 11. Ако је $n = {p_1}^{\alpha_1}{p_2}^{\alpha_2}\cdots{p_k}^{\alpha_k}$ канонска факторизација броја n, онда је

$$\varphi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_k}\right)$$
$$= {p_1}^{\alpha_1 - 1}{p_2}^{\alpha_2 - 1}\cdots{p_k}^{\alpha_k - 1}(p_1 - 1)(p_2 - 1)\cdots(p_k - 1).$$

Доказ. Следи на основу две претходне теореме ($\varphi(n) = \varphi({p_1}^{\alpha_1}{p_2}^{\alpha_2}\cdots{p_k}^{\alpha_k}), \varphi$ мултипликативна, $(p_i, p_j) = 1, i \ne j$, p_i прост број). □
Пример. $\varphi(120) = \varphi(2^3 \cdot 3 \cdot 5) = 2^2 3^0 5^0(2-1)(3-1)(5-1) = 32$
$(\varphi(2^3 \cdot 3 \cdot 5) = \varphi(2^3)\varphi(3)\varphi(5) = 4 \cdot 2 \cdot 4).$
Теорема 12. (Ојлерова теорема) Ако је $(a, m) = 1$, онда је

$$a^{\varphi(m)} \equiv 1(mod\ m).$$

Доказ. $\varphi(m)$ је број природних бројева који нису већи од датог произвољног броја m и узајамно су прости са њим. Нека је $\{\alpha_1, \alpha_2, \dots, \alpha_{\varphi(m)}\}$ сведени систем остатака по модулу $m \overset{\text{т.8}}{\Rightarrow} \{a\alpha_1, a\alpha_2, \dots, a\alpha_{\varphi(m)}\}$ сведени систем остатака по модулу m.
Према томе, за сваки број α_i постоји један и само један број α_j такав да је $a\alpha_j \equiv \alpha_i\ (mod\ m)$ (1). Ако помножимо све конгруенције овог облика, добијамо да је

$$a\alpha_1 a\alpha_2 \cdots a\alpha_{\varphi(m)} \equiv \alpha_1\alpha_2\cdots\alpha_{\varphi(m)}\ (mod\ m), \text{ због (1)}$$
$$a^{\varphi(m)}\alpha_1\alpha_2\cdots\alpha_{\varphi(m)} \equiv \alpha_1\alpha_2\cdots\alpha_{\varphi(m)}\ (mod\ m)$$

Но, пошто је $(\alpha_i, m) = 1,\ i = \overline{1, \varphi(m)}$, то се према теореми 6 може извршити скраћивање , па је

$$a^{\varphi(m)} \equiv 1(mod\ m). \quad \square$$

Задатак 6. Одреди последње две цифре броја 3^{400}.
Решење: Занима нас колики је остатак при дељењу броја 3^{400} са 100, тј.

$$3^{400}(mod\ 100) = ?$$

Критеријуми дељивости за бројеве 4 и 25 имају везе са двоцифреним завршетком: природан број и његов двоцифрени завршетак дају исти остатак при дељењу са 4 и са 25. Занима нас да израчунамо $3^{400}(mod\ 4)$ и $3^{400}(mod\ 25)$.
$(3,4) = 1 \underset{\text{Ојлерова т.}}{\Longrightarrow} 3^2 \equiv 1(mod\ 4)$, па имамо $3^{400} = (3^2)^{400} \equiv 1^{400} \equiv 1(mod\ 4)$.

$(3,25) = 1 \xrightarrow[\text{Ојлерова т.}]{} 3^{20} \equiv 1(mod\ 25)$, па имамо $3^{400} = (3^{20})^{20} \equiv 1^{20} \equiv 1(mod\ 25)$.
Да је број дељив са 25 двоцифрени завршетак би био један од $00,25,50,75$. Да би био дељив и са 4 једини могући јесте 00. Како при дељењу са оба броја имамо остатак један, то је двоцифрени завршетак броја 3^{400} једнак 01. ◊
Овим примером смо видели како нам поменута теорема може помоћи приликом израчунавања.

Теорема 13. („Мала“ Фермаова теорема) Ако је p прост број и p не дели a, онда је
$$a^{p-1} \equiv 1(mod\ p).$$
Доказ.
p прост број и p не дели $a \Longrightarrow \boxed{(a,p) = 1}$
$\boxed{\varphi(p) = p - 1}$ јер је p прост број
Видимо да је ово само специјалан случај већ доказане Ојлерове теореме. □
Задатак 7. Наћи остатак дељења броја 1234^{4321} са 11.
Решење. 11 је прост број, $(1234,11) = 1$ па су испуњени услови теореме 13.
11 прост број $\Longrightarrow \varphi(11) = 10$.
$$1234^{10} \equiv 1\ (mod\ 11)$$
$$1234^{4321} = 1234^{4320} \cdot 1234 = (1234^{10})^{432} \cdot 1234 \equiv 1^{10} \cdot 2\ (mod\ 11)$$
$$1234^{4321} \equiv 2\ (mod\ 11). \quad ◊$$

Последица 2. Ако је p прост број и a произвољан цео број, онда је
$$a^p \equiv a\ (mod\ p).$$
Доказ. За $a = 0$ је $0^p - 0 = 0$ те важи $0^p \equiv 0\ (mod\ p)$ јер је нула дељива са p.
Претпоставимо да важи за $a \in \mathbb{N}$ и докажимо да је то тачно за $a + 1$, тј да важи $p \mid (a+1)^p - (a+1)$.
$$(a+1)^p - (a+1) = \sum_{i=0}^{p} \binom{p}{i} a^{p-i} - a - 1 = a^p + 1 + \sum_{i=1}^{p-1} \binom{p}{i} a^{p-i} - a - 1$$
$$= a^p - a + \sum_{i=1}^{p-1} \binom{p}{i} a^{p-i}.$$
Израз $a^p - a$ је дељива са p по индукцијској претпоставци. Како је $\binom{p}{i} = \frac{p!}{i!(p-i)!}$, $i = \overline{1, p-1}$, бројилац је увек дељив са p, а именилац није (именилац је производ бројева мањих од p који је прост број па га не можемо добити као производ неких чланова), те је $\binom{p}{i}$ дељиво са p.
Дакле, $p \mid a^p - a + \sum_{i=1}^{p-1} \binom{p}{i} a^{p-i}$ (За негативне важи јер $b \mid a \Leftrightarrow b \mid -a$). □

3.5 Примена конгруенција

Као што смо видели код конгруенција бројеви се враћају у круг, након што достигну одређену вредност – модуо.
Најпознатија примена конгруенција је у 24-сатном мерењу времена. Ради се о конгруенцији модуо 24 – бројеви поново почињу од нуле након што достигну 24 (сатови поново почињу од 00 након што прођу 24 сата). Дан траје од поноћи до следеће поноћи, и подељен је на 24 сата, од 0 до 23 ($24 \equiv 0(mod\ 24)$). Ако је у одређеном тренутку 19.00 сати, осам сати касније не износи 27.00 (као код уобичајеног сабирања), већ је тада 03.00 наредног дана ($27 \equiv 3(mod\ 24)$).
На сату се користи конгруенција модуо 12. Ако је 10.00 сати за 4 сата ће бити 14.00 сати, међутим сат је подељен на 12 једнако распоређених тачака, зато се на сату приказује $14 \equiv 2\ (mod\ 12)$ sata.

3.5.1 Критеријуми дељивости

Као једну од примена теорије конгруенција наведимо неколико критеријума дељивости. Један од општијих начина добијања критеријума дељивости је тзв. Паскалов метод. Његова суштина је у следећем: желимо испитати дељивост броја a датим бројем m, што може бити веома компликовано. На основу бројева a и m формирамо нови број b па испитујемо истовремену дељивост бројева a и b бројем m, а што може донети приличне олакшице.
Теорема 14. (Паскалов метод) Да би број $a = \overline{a_n a_{n-1} \dots a_1 a_0} = \sum_{i=0}^{n} a_i \cdot 10^i$ био дељив природним бројем m, неопходно је и довољно да је са m дељив збир $\sum_{i=0}^{n} a_i r_i$, где су r_i произвољни цели бројеви за које важи $10^i \equiv r_i\ (mod\ m)$, $i = \overline{0,n}$.
Напомена: Збир $\sum_{i=0}^{n} a_i r_i$ представља тај нови број b.
Доказ. Доказ је очигледан, јер је $a = \sum_{i=0}^{n} a_i \cdot 10^i \equiv \sum_{i=0}^{n} a_i r_i \ \ (mod\ \ m)$.
А то важи јер:
Теорема 15. Ако је $f(x) = c_0 + \cdots + c_{n-1}x^{n-1} + c_n x^n$ полином са целим коефицијентима $c_i, i = \overline{0,n}$, тада из релације $a \equiv b(mod\, m)$ следи $f(a) \equiv f(b)\ (mod\, m)$.
Доказ. Из $a \equiv b(mod\, m)$, следи $a^i \equiv b^i(mod\, m)$, и $c_i a^i \equiv c_i b^i(mod\, m), i = \overline{0,n}$.
Такође

$$c_n a^n + c_{n-1}a^{n-1} + \cdots + c_o \equiv c_n b^n + c_{n-1}b^{n-1} + \cdots + b_0(mod\, m)$$

тј.

$$f(a) \equiv f(b)\ (mod\, m). \quad \square$$

Пример. Испитајмо да ли је број 24 804 дељив бројем 36 користећи Паскалов критеријум.
Решење. Означимо $a = 24\,804 = 4 \cdot 10^0 + 0 \cdot 10^1 + 8 \cdot 10^2 + 4 \cdot 10^3 + 2 \cdot 10^4$
Одавде следи да је: $10^0 = 1 \equiv 1 \ \ (mod\ \ 36)$,

$$10^1 \equiv 10 \ \ (mod\ \ 36)$$
$$\dots.$$
$$10^4 \equiv 28 \ \ (mod\ \ 36),$$

(односно $a \equiv 4 \cdot 1 + 0 \cdot 10 + 8 \cdot 28 + 4 \cdot 28 + 2 \cdot 28 \ \ (mod\ \ 36)$) ,
тј.

$$b = 4 \cdot 1 + 0 \cdot 10 + 8 \cdot 28 + 4 \cdot 28 + 2 \cdot 28 = 396.$$

Према Паскаловом критеријуму, ако је број $b = 396$ дељив бројем 36, онда је и број $a = 24804$ дељив бројем 36. Овим смо добили мањи број као дељеник. Поступак можемо користити итеративно с тим што улогу броја a преузима број b:

$$b = 396 = 6 \cdot 1 + 9 \cdot 10 + 3 \cdot 100 \equiv 6 + 9 \cdot 10 + 3 \cdot 28 \ \ (mod\ \ 36)$$

$$b_1 = 6 + 9 \cdot 10 + 3 \cdot 28 = 180$$
$$b_1 = 180 = 0 + 8 \cdot 10 + 1 \cdot 100 \equiv 0 + 8 \cdot 10 + 1 \cdot 28 \pmod{36}$$
$$b_2 = 0 + 8 \cdot 10 + 1 \cdot 28 = 108$$
$$b_2 = 108 = 8 + 0 \cdot 10 + 1 \cdot 100 \equiv 8 + 0 \cdot 10 + 1 \cdot 28 \pmod{36}$$
$$b_3 = 8 + 0 \cdot 10 + 1 \cdot 28 = 36$$

Како број $b_3 = 36$ јесте дељив са 36, то је и број $a = 24804$ дељив са 36. ◊

С обзиром да се сваки природан број може приказати у облику производа степена простих бројева, од интереса је да се добију критеријуми дељивости степенима простих бројева.

Бирајући на одговарајући начин бројеве r_i, добијају се разни критеријуми дељивости. Најчешће се за бројеве r_i узимају остаци при дељењу бројева 10^i са m.

Последица 3. Нека је t такав број да је $10^t \equiv 1 \pmod{m}$. Да би број a био дељив са m, неопходно је и довољно да је са m дељив збир бројева који се добијају поделом здесна налево броја a на групе по t цифара.

Специјално, одавде добијамо познате критеријуме дељивости са 3, 9 и 11:

а) $10^1 \equiv 1 \pmod{3} \Rightarrow t = 1$, тј. број a делимо на једноцифрене бројеве и посматрамо њихов збир.

Дакле, дати број a запишимо у облику $a = \overline{a_n \dots a_1 a_0} = a_0 + a_1 \cdot 10^1 + \cdots + a_n \cdot 10^n$,

Како је $10^i \equiv 1 \pmod{3}$ $i = \overline{0,n}$, то важи $a \equiv a_0 + a_1 + \cdots + a_n \pmod{3}$ (што представља збир цифара броја a и то је број b из Паскаловог критеријума) , па важи:

$$\boxed{\mathbf{3} \mid a \Leftrightarrow \mathbf{3} \mid a_n + \cdots + a_1 + a_0.}$$

б) $10^1 \equiv 1 \pmod{9} \Rightarrow t = 1$

Аналогно се показује да важи: $\boxed{\mathbf{9} \mid a \Leftrightarrow \mathbf{9} \mid a_n + \cdots + a_1 + a_0}$

в) $10^2 \equiv 1 \pmod{11} \Rightarrow t = 2$, тј. број a делимо на бројеве од по две цифре.

Запишимо број a у систему са основом 100, тј. $a = \overline{a_n \dots a_1 a_0} = \overline{a_1 a_0} + \overline{a_4 a_3} \cdot 100 + \overline{a_6 a_5} \cdot 100^2 + \cdots$

Како је $10^i \equiv 1 \pmod{11}$ $i = \overline{2,n}$, то важи $a \equiv \overline{a_1 a_0} + \overline{a_4 a_3} + \overline{a_6 a_5} + \cdots \pmod{11}$.

Дакле, важи следеће правило: $\boxed{\mathbf{11} \mid a \Leftrightarrow \mathbf{11} \mid \overline{a_1 a_0} + \overline{a_4 a_3} + \overline{a_6 a_5} + \cdots}$

Последица 4. Нека је t такав број да је $10^t \equiv -1 \pmod{m}$. Да би број a био дељив са m, неопходно је и довољно да је са m дељив збир бројева који се добијају поделом здесна налево броја a на групе по t цифара, али им се наизменично мења знак.

Специјално, одавде добијамо једноставнији критеријум дељивости са 11 и критеријум дељивости са 7:

а) $10^1 \equiv -1 \pmod{11} \Rightarrow t = 1$, тј. број a делимо на једноцифрене бројеве и посматрамо њихов збир.

$$a = \overline{a_n \dots a_1 a_0} = a_0 + a_1 \cdot 10^1 + \cdots + a_n \cdot 10^n$$
$$\equiv a_0 \cdot 1 + a_1 \cdot (-1) + a_2 \cdot 1 + \cdots \pmod{11}$$

Добили смо други критеријум за дељивост бројем 11:

$$\boxed{\begin{array}{c} \mathbf{11} \mid a \Leftrightarrow \mathbf{11} \mid a_0 - a_1 + a_2 - a_3 + \cdots \quad \text{тј.} \\ \mathbf{11} \mid a \Leftrightarrow \mathbf{11} \mid (a_0 + a_2 + \cdots) - (a_1 + a_3 + \cdots) \end{array}}$$

б) $10^3 \equiv -1 \pmod{7} \Rightarrow t = 3$, тј. број a делимо на троцифрене бројеве и посматрамо њихов збир.

$$a = \overline{a_n \dots a_1 a_0} = \overline{a_2 a_1 a_0} \cdot 1000^0 + \overline{a_5 a_4 a_3} \cdot 1000^1 + \cdots$$
$$\equiv \overline{a_2 a_1 a_0} \cdot 1 + \overline{a_5 a_4 a_3} \cdot (-1) + \cdots \pmod{7}$$

Дакле, важи: $\boxed{\mathbf{7} \mid a \Leftrightarrow \mathbf{7} \mid \overline{a_2 a_1 a_0} - \overline{a_5 a_4 a_3} + \cdots}$

Задатак. Доказати да важи:
1° Број $a=\overline{a_n\dots a_1a_0}$ је дељив са 27 $\Leftrightarrow \overline{a_3a_2a_1}+\overline{a_6a_5a_4}+\overline{a_9a_8a_7}+\cdots$ је дељиво са 27.
2° Број $a=\overline{a_n\dots a_1a_0}$ је дељив са 13 $\Leftrightarrow \overline{a_3a_2a_1}-\overline{a_6a_5a_4}+\overline{a_9a_8a_7}-\cdots$ је дељиво са 13.
3° Број $a=\overline{a_n\dots a_1a_0}$ је дељив са 37 $\Leftrightarrow \overline{a_3a_2a_1}+\overline{a_6a_5a_4}+\overline{a_9a_8a_7}+\cdots$ је дељиво са 37.
Решење. 1° $10^3\equiv 1 \pmod{27}$,

$$a=\overline{a_n\dots a_1a_0}=\overline{a_3a_2a_1}\cdot 1000^0+\overline{a_6a_5a_4}\cdot 1000^1+\overline{a_9a_8a_7}\cdot 1000^2+\cdots$$
$$a\equiv \overline{a_3a_2a_1}+\overline{a_6a_5a_4}+\overline{a_9a_8a_7}+\cdots \pmod{27}.$$

1° $10^3\equiv -1 \pmod{13}$;
2° $10^3\equiv 1 \pmod{37}$. ◊

Последица 5. Да би за неко $t\in\mathbb{N}$ број $a=\overline{a_n\dots a_1a_0}$ био дељив са 2^t (односно 5^t), неопходно је и довољно да је са 2^t (односно 5^t) дељив број $\overline{a_{t-1}\dots a_1a_0}$ (t-оцифрени завршетак).

Из овог добијамо критеријуме дељивости бројевима 2, 4, 8, 16…(степени двојке) и критеријуме дељивости бројевима 5, 25, 125…(степени броја 5):

Дати број a запишимо у облику $a=\overline{a_n\dots a_1a_0}=a_0\cdot 10^0+a_1\cdot 10^1+\cdots+a_n\cdot 10^n$.

Дељивост са 2:

Како је $10\equiv 0(mod\ 2)$ то је према последици 1, $10^i\equiv 0(mod\ 2), i=\overline{1,n}$.
То је

$$a\equiv a_0\cdot 1+a_1\cdot 0+\cdots+a_n\cdot 0 \pmod{2},$$
$$a\equiv a_0 \pmod{2}, \text{тј.}$$

Број је дељив бројем **2** акко је једноцифрени завршетак дељив са **2**.

Јер, ако је лева страна конгруентна нули по модулу 2, онда мора бити и десна страна, а то је једино могуће ако је последња цифра a_0 тог броја дељива са 2.

Дељивост са 4:

$10^2\equiv 100\equiv 0\ (mod\ 4)$, па је $100^i\equiv 0\ (mod\ 2^2), i=\overline{1,n}$
$$a\equiv a_0\cdot 1+a_1\cdot 10+a_2\cdot 0+\cdots+a_n\cdot 0 \pmod{2^2},$$
$$a\equiv a_0+a_1\cdot 10 \pmod{2^2}, \text{тј. } a\equiv \overline{a_1a_0}\ (mod\ 2^2).$$

Број је дељив бројем $\mathbf{2^2}$ акко је двоцифрени завршетак дељив са $\mathbf{2^2}$.

Дељивост са 5:

$10\equiv 0\ (mod\ 5)$, па је $10^i\equiv 0\ (mod\ 5), i=\overline{1,n}$.
$$a\equiv a_0\cdot 1+a_1\cdot 0+\cdots+a_n\cdot 0 \pmod{5},$$
$$a\equiv a_0\ (mod\ 5).$$

Број је дељив бројем **5** акко је једноцифрени завршетак дељив са **5**, тј. акко је последња цифра **0** или **5**.

Уопштено, довољно је у теореми 13 узети $r_i=10^i$ за $i=\overline{0,t-1}$ и $r_i=0$ за $i\geq t-1$

Критеријум дељивости са 10:

Како је $10\equiv 0(mod\ 10)$ то је према последици 1, $10^i\equiv 0(mod\ 10), i=\overline{1,n}$.
Из тога имамо

$$a=\overline{a_n\dots a_1a_0}=a_0\cdot 10^0+a_1\cdot 10^1+\cdots+a_n\cdot 10^n\equiv a_0(mod\ 10)$$

Дакле $a\equiv a_0(mod\ 10)$, па је

број a дељив са 10 акко му је последња цифра дељива са 10, односно акко му је последња цифра једнака 0.

Задатак 8. Докажи да је палиндром с парним бројем цифара дељив са 11.

Решење. Нека ја $a = \overline{a_n a_{n-1} \dots a_1 a_0}$ палиндром са парним бројем цифара. Пошто је у питању палиндром за цифре важи $a_n \equiv a_0, a_{n-1} \equiv a_1, a_{n-2} \equiv a_2$ ... и како има паран број цифара разлика цифара на парним и непарним местима биће

$$(a_0 + a_2 + \cdots + a_{n-1}) - (a_n + a_{n-2} + \cdots + a_1) = 0.$$

Па

$$11 \mid (a_0 + a_2 + \cdots + a_{n-1}) - (a_n + a_{n-2} + \cdots + a_1), \text{ тј. } 11 \mid a. \quad \Diamond$$

3.5.2 Round-robin турнир

Споменимо сада и једну учесталу примену конгруенције у свету спорта.
Претпоставимо како је потребно направити распоред сусрета у турниру који се састоји од n играча или тимова на такав начин да сваки играч или тим игра са сваким другим тачно једном. Турнир који се одиграва према такво распореду назива се round-robin турнир.
Како имамо n играча то ће на турниру бити $n-1$ кола, сваки играч се састаје са сваким другим тачно једном па би сваки играч требао наступити у сваком колу. Ако имамо паран број тимова, у једном колу сваки тим има пара, али ако је број тимова непаран тада немају сви тимови свој пар. У том случају додајемо још један, фиктиван, тим и можемо претпоставити да је n паран. Наравно, тим који се састаје с фиктивним тимом у неком колу је у ствари слободан у том колу. Турнир се састоји од укупно $n-1$ кола, у сваком колу игра $\frac{n}{2}$ парова, те ће бити $\frac{(n-1)n}{2}$ утакмица.
Означимо тимове с $1,2,3,\dots,n$. У k–том колу, тимови x и $y, 1 \le x, y \le n-1, x \ne y$, играју међусобно уколико је $x + y \equiv k(mod\ n-1)$. Уколико је $x + x \equiv k(mod\ n-1)$, тада тим x игра с тимом n.
Пример. Направимо распоред турнира за 5 тимова. Имамо два пара тако да додајемо један фиктиван тим да сви тимови имали пара. Обележимо играче 1,2,3,4,5,6.
Прво коло: играју међусобно ако $x + y \equiv 1(mod\ 5)$, тј. парови су: 1-5; 2-4; 3-6 јер $3 + 3 \equiv 1(mod\ 5)$ па тим 3 игра с тимом 6, тј. тим је у првом колу слободан, ако смо бројем 6 означили фиктивни тим. Тако наставимо даље и добијамо распоред за турнир дат следећом табелом.

Тим / Коло	1	2	3	4	5
1	5	4	слободан	2	1
2	слободан	5	4	3	2
3	2	1	5	слободан	3
4	3	слободан	1	5	4
5	4	3	2	1	слободан

Ако избацимо фиктивне утакмице имамо 10 утакмица у 5 кола, сваки тим игра по 4 утакмице и сваки тим игра само једном у датом колу. ◊
Приметимо како ни један тим неће играти више од једног пута у истом колу, јер ако играч x у истом колу k игра са два различита играча y и z биће

$$x + y \equiv k(mod\ n-1) \text{ и } x + z \equiv k(mod\ n-1), \text{ тј.}$$
$$x + y \equiv x + z(mod\ n-1),$$
$$y \equiv z(mod\ n-1)$$

те је $y = z$ због $1 \le y, z \le n-1, y \ne z$.
Такође неће доћи до понављања сусрета у колима: нека су k и k_1 различита кола, из $x + y \equiv k(mod\ n-1)$ и $x + y \equiv k_1(mod\ n-1)$ следи $k \equiv k_1(mod\ n-1)$, тј. $k = k_1$ због $1 \le k, k_1 \le n-1$.

3.5.3 Модуларни дизајни

Конгруенције се могу користити за креирање различитих дизајна. Овде ћемо показати како се креира звезда са m врхова.
На кружници произвољног полупречника означимо m једнако удаљених тачака и означимо их с $0,1,\dots,m-1$. Изаберимо r - произвољан најмањи остатак по модулу m али такав да важи $(m,r)=1$. Спојимо сваку x тачку с тачком $(x+r)\ (mod\ m)$.
Пример. Конструишимо звезду са 10 врхова.
На кружници обележимо 10 једнако удаљених тачака бројевима од 0 до 9 (правилан десетоугао). Узмимо на пример, $r=3$.

x	0	1	2	3	4	5	6	7	8	9
$x+3$	3	4	5	6	7	8	9	10	11	12
$(x+3)(mod\ 10)$	3	4	5	6	7	8	9	0	1	2

Односно спојимо тачку 0 с тачком 3, 1 са 4,…, 8 са 1 и тачку 9 и тачку 2.

3.5.4 Криптографија-RSA алгоритам[3]

Један од важних проблема у криптографији је тзв. проблем дистрибуције кључа. Наиме, да би две особе, А и Б, размењивале шифроване поруке, претходно треба да размене одређену информацију (број) која се зове кључ и помоћу које се шифровање врши. Дуго се сматрало да исти број треба да служи и за шифровање и за дешифровање, тј. да треба обе особе да га знају, па је постојао проблем безбедног преноса те информације. Седамдесетих година 20. века дошло се на идеју која чини такав пренос непотребним, а која користи Ојлерову теорему.

У овом алгоритму кључну улогу имају велики прости бројеви; сигурност алгоритма заснива се на сложености факторизације великих бројева. За дешифровање је потребно знати тајни број d. Он се рачуна помоћу $\varphi(N)$, а за израчунавање тог броја потребно је знати p и q- бројеви који нису јавни ($\varphi(N)$ не можемо наћи само на основу броја N). Како само особа А зна број d, само она може и дешифровати.

Један могући поступак је дат на следећој страни.

[3] Творци овог алгоритма су Роналд Риверс, Леонард Ејдлман и Ади Шамир, где RSA(Rivest-Shamir-Adleman) представља акроним њихових имена.

Особа А: - Бира два врло велика проста броја p и q; - Рачуна: $N = pq;$ $\varphi(N) = \varphi(p)\varphi(q) = (p-1)(q-1);$ - Бира произвољан број e који задовољава услов $(e, \varphi(N)) = 1$; - Налази број d који задовољава линеарну конгруенцију $de \equiv 1(mod\ \varphi(N))$; - Особа А објављује (нпр. стављањем на сајт) бројеве N и e. Број d не објављује.	- Бира $p = 7, q = 11$(због примера бирамо мале бројеве) - $N = 7 \cdot 11 = 77, \varphi(N) = 6 \cdot 10 = 60$ - $(e, 60) = 1$, нпр. $e = 13$. - Рачуна број d (применом Еуклидовог алгоритма, бирали да буду узајамно прости): $13d \equiv 1(mod\ 60),$ постоји број $t, 13d + 60t = 1,$ $60 = 13 \cdot 4 + 8$ .... $\underbrace{-23}_{37(mod\ 60)} \cdot 13 + 60 \cdot 5 = 1,$ $d = 37.$ -Објављује N и e.
Особа Б: Жели да пошаље поруку и нека је x део текста који треба шифровати; шифрује је тако што рачуна остатак y при дељењу броја x^e са N, тј. $x^e \equiv y(mod\ N).$ Шифрована порука је y. Узимамо да је x строго мањи од N.	Претпостављамо да се користи алфабет. Сваком од 26 слова можемо придружити његов одговарајући редни број умањен за 1, тј. слову А одговара 0,…,слову Z одговара 25. Нека порука гласи ТВ. Када узмемо позиције слова у абецеди добијамо 202 (Т-20, В-2). Текст растављамо на два дела од којих ћемо сваки шифровати посебно. Растављамо на 20 и 2 како би били мањи од 77. Шифрује: $20^{13} \equiv 69(mod\ 77), 2^{13} \equiv 30(mod\ 77).$ Према томе, шифровани текст је 69 30.
Особа А За дешифровање користи само њој познат број d тако што рачуна остатак при дељењу броја y^d са N. Наиме, важи $y^d \equiv (x^e)^d = x^{de} = x^{\overbrace{t\varphi(N)+1}^{de \equiv 1(mod\ \varphi(N))}} \equiv x\ (mod\ N),$ јер је, према Ојлеровој теореми, $x^{\varphi(N)} \equiv 1\ (mod\ N)$ (услов $(x, N) = 1$ може се сматрати испуњеним јер је $x < N$ које је производ два велика проста броја).	Рачуна $69^{37}(mod\ 77)$ и $30^{37}(mod\ 77).$ Наравно, дешифровањем добијамо 20 2.

ЛИТЕРАТУРА

1. Владимир Мићић, Зоран Каделбург, Душан Ђукић, „Увод у теорију бројева“, Друштво математичара Србије, Београд, 2013.
2. Математички лист X – 5, Друштво математичара Србије, Београд, 1976.
3. Осјечки математички лист 11(2011), бр. 2, Осијек, 2011.
4. Војко Несторовић, „Бројевне конгруенције“, Мастер рад, Природно- математички факултет, Нови Сад, 2011.
5. Ирена Ужар, „Примена конгруенција“, Дипломски рад, Свеучилиште J.J. Strossmayera, Осијек, 2016.
6. Иван Матић, „Увод у теорију бројева“, скрипта, Осијек, 2016.
7. Андреј Дујела, „Увод у теорију бројева“, скрипта, Загреб, 2002.
8. Небојша Икодиновић, Слађана Димитријевић, Сања Милојевић, Ненад Вуловић, „Приручник за наставнике“, Клет, Београд, 2009.
9. Светлана Јоксимовић, „Математика- уџбеник са радним листовима 1,2,3,4“, Едука, Београд, 2015.
10. http://srb.imomath.com/index.php?options=31&lmm=1
11. http://www.np.ac.rs/downloads/nm/nm_mat/diskret_mat.pdf